LiNUX+

LA MAYOR REVISTA ONLINE SOBRE LINUX

Nº4/2010 (64) MENSUAL ISSN 1732-7121

INFORMÁTICA FORENSE Y SOFTWARE LIBRE

PONIENDO EN MARCHA UNA ESTACIÓN DE TRABAJO CON SLACKWARE 13.0

HACHOIR
FRAMEWORK PARA MANIPULAR ARCHIVOS BINARIOS

ENDIAN FIREWALL
UN CORTAFUEGOS PARA TODOS LOS PÚBLICOS

SDL.NET
INTRODUCCIÓN AL DESARROLLO DE VIDEOJUEGOS

DE CLAROLINE A MENTOR
ADAPTACIÓN DE UNA PLATAFORMA DE E-LEARNING EN UN CENTRO EDUCATIVO

MAEMO 5
LA APUESTA DE NOKIA POR EL SOFTWARE LIBRE

La dulce vida sin jefe

Ya estamos en abril y con este nuevo mes os entregamos nuevo número de Linux+ con una serie de artículos fresquitos. En parte lo dedicamos a informática forense que es un tema que despierta mucha curiosidad últimamente. Otro tema de interés que tratamos en este número es la plataforma Maemo de Nokia, y lo que nos ofrece. Y como siempre encontraréis artículos dedicados a programación y seguridad, dos temas muy importantes en nuestros tiempos.

Cambiando un poco el tema, ¿habéis pensado alguna vez cómo sería la vida sin un jefe diciéndonos qué tenemos que hacer? ¿Sin tener que realizar las ideas de alguien, y de la manera pensada por alguien?

> *“¿Habéis pensado alguna vez cómo sería la vida sin un jefe diciéndonos qué tenemos que hacer? Pues yo si (y mucho)...”*

Pues yo si (y mucho), y supongo que habrá más personas soñando con que un día se despierten y no habrá un superior en su vida. Por eso a partir del próximo número queremos animaros a probar vuestras fuerzas para desarrollar vuestro propio negocio en internet y aprovechar las oportunidades que nos ofrece linux en este campo. Para ello vamos a publicar artículos y entrevistas con las personas emprendedoras que se ganan la vida gracias a sus propias ideas y conocimientos sin contar con mucho presupuesto para el negocio. Queremos publicar historias interesantes que os inspiren y animen a probar vuestra suerte en el mercado.

Si ya tenéis vuestro propio negocio en internet y creéis que vuestra historia puede ser una inspiración para otros lectores, escribidnos a *es@lpmagazine.org* y muy posiblemente la presentemos en Linux+. ¡Esperamos vuestras experiencias!

Y para terminar no me queda más que desearos Felices Pascuas, que descanséis y que la primavera que acaba de llegar os ponga de buen humor.

¡Buena lectura y hasta el mayo!

Paulina Pyrowicz
Redactora Jefe de Linux+

En este número

novedades

cómputo forense

Instalar Slackware, después de haber conocido distribuciones como Fedora, SuSE o Ubuntu, es como una especie de dejà vú. ¿Qué te voy a contar precisamente a ti, que a finales de los 90 conociste Linux gracias a esta distro -ahora en su versión 13.0? Fuiste de los que la hacían arrancar en modo de emulación con UMSDOS. Instalaste aquella cosa y contra todo pronóstico funcionó. Experimentaste con ella. A golpe de editor configuraste las X y las obligaste a escribir eñes y tildes hackeando librerías del sistema con un parche descargado de Internet.

Cuando se realiza análisis forense, una de las fases en la metodología forense, es inherente trabajar con archivos binarios. Hachoir es la palabra francesa utilizada para un picador de carne, el cual es utilizado por los carniceros para dividir la carne en secciones largas. Hachoir es utilizado por los carniceros en cómputo forense para dividir los archivos binarios en campos. De esta manera permite visualizar y editar campo por campo flujos binarios o secuencias binarias.

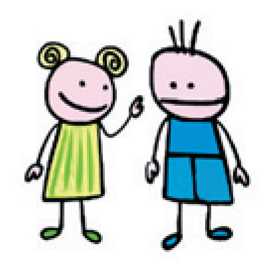
proyectos open source

Hasta hace poco tiempo, tener completamente integrado el SO del pingüino en un dispositivo portátil (teléfono móvil, pda, etc.) era algo que requería bastante esfuerzo y en gran parte de los casos, por no decir la mayoría, era impensable. Actualmente encontramos varios intentos en el mercado de querer integrar de manera eficiente el SO Linux en este tipo de dispositivos. Pero, si deseamos tener integrado en un solo dispositivo una cámara, un GPS, teclado "qwerty", acelerómetros, teléfono móvil, e Internet gestionados por Linux de manera eficiente, solamente podemos pensar en el binomio Maemo + Nokia.



Tema del número **Cómputo forense**







Ubuntu One Music Store abre sus puertas al público

Los desarrolladores de Canonical habían mantenido una fase en beta privada para su tienda de música online hasta la fecha, y por fin podemos disfrutar de este proyecto que ha abierto sus puertas a todos los usuarios. La tienda ya dispone de acceso al catálogo de 7Digital, el partner de Canonical en esta iniciativa, y en dicho catálogo disponemos tanto de canciones de pago como de música gratuita gracias a las páginas especialmente dedicadas a este servicio. Uno de los aspectos que se han tenido en cuenta en la puesta en marcha de este servicio es la geolocalización de los internautas y usuarios de Ubuntu que se conectan a la tienda. Gracias al estudio de la IP se nos proporcionará automáticamente acceso a la versión de la tienda que nos corresponde según nuestra localización, y que puede dividirse en cinco grandes grupos: Reino Unido, Estados Unidos, Alemania, Resto de Europa (sin Alemania o Reino Unido) y Resto del mundo (exceptuando todos los países anteriores).
Ya podéis probar el servicio, aunque como ya comentamos necesitaréis una cuenta en el servicio Ubuntu One de Canonical que actúa como almacén intermedio para esas canciones.
http://www.muylinux.com/2010/03/23/ubuntu-one-music-store-abre-sus-puertas-al-publico/

NanoNote, la sub-netbook de US$ 99 totalmente libre y abierta

Qi Hardware, un nueva empresa que incluye a antiguos miembros del proyecto OpenMoko, comenzó a vender por sólo US$ 99 el ultraportátil dispositivo Ben NanoNote, una mezcla de UMPC, PDA, palmtop y smartbook de bajo nivel. La NanoNote, con un mínimo display TFT de 3" (320x240 píxeles), incluye un CPU Jz4720 compatible con MIPS de 336 MHz, 32 Mb de SDRAM y 2 Gb de memoria flash NAND, además de un conector de expansión microSDHC. En sus reducidísimas dimensiones de 99 x 75 x 17,5 mm puede acomodar un teclado QWERTY y una batería de litio-ion de 850 mAh, pesando sólo 126 gramos.
Pero lo mejor de todo es que toda la NanoNote es completamente abierta: sus especificaciones de hardware están disponibles con una licencia copyleft y usa la distribución OpenWrt con un Kernel 2.6, amparada bajo la GPL, por supuesto. Qi Hardware espera de esta manera atraer a los "hackers" más inquietos y al mismo tiempo usar a la NanoNote para construir progresivamente una línea de netbooks y smartphones.
Es destacable que esta "democratización del diseño del hardware" es realmente completa: no solo se publican las especificaciones y los esquemas de la NanoNote, sino también los próximos planes para su software y hardware.
http://www.vivalinux.com.ar/hard/ben-nanonote

SUSE Linux triunfa gracias al acuerdo Novell-Microsoft

Del tan criticado acuerdo de colaboración realizado en noviembre de 2006 entre Novell y Microsoft para hacer interoperables sus respectivos sistemas operativos, se han cosechado grandes éxitos durante estos más de tres años, logrando por ejemplo operaciones en España en compañías como BBVA, Generalitat de Catalunya, Endesa o Prisa que implican a decenas de miles de servidores con SUSE Linux, convirtiendo paradójicamente a Microsoft en el mayor vendedor de SUSE Linux.

José Manuel Enríquez, director general de Novell, desveló algunos detalles de esta sorprendente alianza entre los propietarios de dos de los principales sistemas operativos usados en entornos empresariales. El marco de partida de este acuerdo firmado a finales de 2006 es que en el 70% de los servidores instalados conviven distribuciones Linux con Windows. Esto y la tendencia a virtualizar todo tipo de entornos hicieron de la necesidad de convivir una oportunidad de mercado.

Y los resultados de este acuerdo de cooperación a largo plazo ya son medibles: 36 contratos firmados en España con grandes organizaciones (200 contrataciones y 60.000 certificados de soporte en toda Europa), decenas de miles de servidores que se benefician de la interoperabilidad, intercambio de patentes para lograr el mayor grado de entendimiento entre SUSE y Windows (se consigue incluso la virtualización inversa: operar Linux desde Windows o Windows desde Linux).

Para José Antonio Laguna, el máximo responsable de Microsoft de este acuerdo, su compañía tenía dos caminos: no hacer nada y centrarse en Windows o colaborar con el mundo Linux de una forma profesional. De ahí la elección de Novell que, junto con Red Hat, se reparten el mercado Linux de pago.

La colaboración es total. De hecho, Microsoft ha renovado la compra de certificados de SUSE por valor de cien millones de dólares y los vende directamente a sus clientes. Y la promoción es conjunta. Además, Novell ofrece a los clientes de Microsoft soporte extendido a otras distribuciones Linux como Red Hat. En este terreno empresas como Santa Lucia o Portugal Telecom se están beneficiando del soporte técnico de Novell.

Competencia entre Office y OpenOffice.org

Eso sí, la alianza de Novell y Microsoft no es total. En otro frente, en el de OpenOffice.org, Novell compite a muerte contra el gigante Office. De hecho, actualmente -de la mano de Movistar- tiene una oferta destinada a pymes en la que oferta una licencia de mantenimiento de esta popular suite por 2,5 euros por mes y puesto de trabajo. "Pero en lo que sí estamos trabajando es en un mayor entendimiento entre los formatos ODF y XML", comenta Enríquez, director general de Novell.

http://microteknologias.wordpress.com/2010/03/17/suse-linux-triunfa-gracias-al-acuerdo-novell-microsoft/

Linux 2.6.33 viene con una mejora importante para netbooks y móviles

Aunque se esperaba para los primeros días de marzo, la nueva versión del núcleo Linux numerada como 2.6.33 ya fue publicada oficialmente, veamos cuáles son algunas de las mejoras más interesantes.

Esta versión incluye por primera vez la integración del driver de código abierto Nouveau para chips gráficos Nvidia. Recordemos que estos drivers fueron desarrollados por la comunidad de código abierto sin apoyo de la compañía y a pesar de la complejidad del proyecto por no contar con información sobre cómo funcionan estos chips, ya se cuenta con un grado de madurez que lo hace usable para tareas básicas, evitando la necesidad de descargar el driver cerrado de Nvidia.

Se ha agregado DRBD. Se trata de un esquema de almacenamiento distribuido para aplicaciones que requieren alta disponibilidad. Es un esquema muy similar a algo que se conoce como RAID-1 en donde se tienen varios discos con información



duplicada, si falla un disco, simplemente se reemplaza mientras el otro sigue funcionando. Con DRBD los discos están separados físicamente y la sincronización se realiza a través de la red.

Linux cuenta con un mecanismo llamado ftrace para monitorear el sistema en forma no intrusiva. Se puede pensar como un mecanismo que permite enchufarse a una funcionalidad del sistema para ver qué está haciendo. En esta versión se han agregado utilidades para obtener información acerca del rendimiento del sistema.

Se incluye TCP Cookie Transactions. Se trata de un mecanismo para evitar ataques de denegación de servicio. Una técnica usual en este tipo de ataques es solicitar una gran cantidad de conexiones al mismo tiempo (SYN Flood), lo que hace que el servidor trate de atenderlas porque no tiene cómo distinguir cuales son realmente válidas. Con TCPCT se establece una negociación para asegurar que quien pide la conexión sea un cliente válido.

En la versión anterior se incluyó KSM para mejorar el uso de memoria en sistemas virtualizados. Una debilidad de esta ingeniosa idea era que las páginas de memoria compartidas no se podían llevar a disco cuando se necesitaba más memoria. Esta limitación ha sido eliminada con esta nueva versión.

Ahora que el kernel se encarga de los detalles de bajo nivel del sistema gráfico a través de kernel mode setting, se ha incluido como funcionalidad universal una llamada al sistema para sincronizar las aplicaciones con el refresco de la pantalla. Esto significa que ahora las aplicaciones o bibliotecas gráficas podrán saber cuándo es el mejor momento para actualizar lo que está dibujado en pantalla sin riesgo de que se dibuje parcialmente durante un cuadro, causando el famoso efecto de tearing.

Esta es una funcionalidad que siempre se pidió pero no había un acuerdo sobre cómo implementarla. En sistemas antiguos que no eran multitarea era increíblemente simple de implementar, pero en sistemas multitarea y con el gran desorden que existía en el mundo de los drivers antes de *kernel-mode-setting*, el desafío era bastante grande.

Y finalmente el cambio más interesante para los netbooks y teléfonos móviles. Al

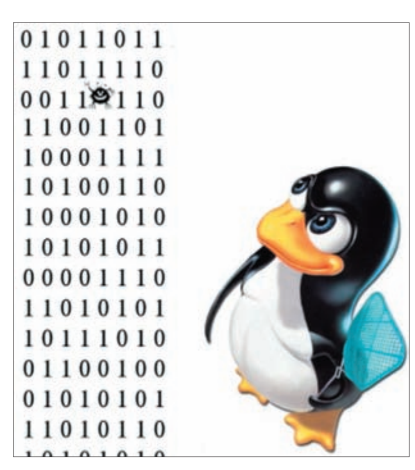


Figura 1. La nueva versión del núcleo Linux numerada como 2.6.33 ya fue publicada oficialmente, y viene con mejoras importantes para netbooks y móviles

esquema de swapping o intercambio existente, incluyendo la unificación de páginas de memoria con contenido repetido, se ha agregado un paso intermedio de compresión. En vez de ir directamente al disco, ahora el swap se podrá hacer a un dispositivo virtual que comprime las páginas de memoria no utilizadas en RAM sin necesidad de llevarlas al disco, mejorando considerablemente el rendimiento por no tener que recurrir a un disco físico cuando la memoria se hace escasa.

¿Qué tan bueno es? Se han realizado varios benchmarks en donde sólo se ha encontrado un caso en donde no trae beneficios. En estos benchmarks destacan aquellos en donde se han detectado tasas de compresión de 4:1, o bien, una reducción de un 25% de la memoria necesaria para usar el sistema. Por ejemplo si tu entorno de escritorio junto a las aplicaciones requieren 256MB de RAM, ahora sólo necesitarán 64MB de RAM.

Si esto no te parece impresionante, también se puede ver desde el punto de vista del rendimiento. Se hicieron pruebas al realizar tareas rutinarias con el mecanismo estándar de swap a disco, usando un disco de 10.000 RPM y se obtuvo un promedio de 200-300 milisegundos ocupados en swap, con el nuevo sistema, estos tiempos bajan a sólo 10 milisegundos.

http://www.fayerwayer.com/2010/02/linux-2-6-33-viene-con-una-mejora-importante-para-netbooks-y-moviles/

Ex Chief Open Source Officer de Sun ahora es miembro del Directorio de Open Source Initiative

Simon Phipps, quien renunciará este martes al puesto de Chief Open Source Officer en Sun, ha sido nombrado miembro del Directorio de Open Source Initiative (OSI), la organización que definió el concepto de Open Source (o Código Abierto) a través de Open Source Definition, una referencia que aún se mantiene vigente.

Aunque fue nombrado hoy, iniciará sus actividades el 1º de abril en esta organización que aun juega un rol muy relevante e importante en el mundo de la libertad del Software. Segun Phipps, las políticas de gobierno y empresas respecto al código abierto utilizan el Open Source Definition de OSI como el estándar sobre qué significa código abierto y OSI actúa como una autoridad enfrentando a los que abusan del término.

Además indica que OSI ha hecho algunos cambios a la forma en que se aprueban las licencias en respuesta a las críticas de que era muy fácil que una licencia fuera calificada como de código abierto lo que provocó una proliferación de licencias diferentes.

http://www.fayerwayer.com/2010/03/ex-chief-open-source-officer-de-sun-ahora-es-miembro-del-directorio-de-open-source-initiatiative/

DELL mira "fuera" de China

La censura china y el caso Google estaría forzando al segundo fabricante mundial de ordenadores a "buscar entornos más seguros fuera de China", escriben desde el diario Hindustan Times citando al primer ministro indio. Los ejecutivos de Dell reevaluarían la dependencia de China y 25.000 millones de dólares en compras de distintos componentes saldrían fuera del país "buscando entornos jurídicos más seguros".

http://www.muycomputerpro.com/Actualidad/Noticias/Dell-mira-fuera-de-China

Mozilla extiende su herramienta de seguridad a IE, Safari , Chrome y Opera

Mozilla está preparando una herramienta que da a los usuarios de los navegadores rivales, incluido Internet Explorer (IE), Chrome, Safari y Opera, una manera de comprobar que los complementos, o añadidos, están actualizados.

La herramienta, un complemento de un mecanismo de control integrado en Firefox 3.6, permite que los usuarios de Chrome 4, Opera 10.5 y Safari, comprueben la antigüedad de sus plugins, como por ejemplo Adobe Flash o Apple QuickTime, que frecuentemente son objetivo de los hackers. El soporte para Internet Explorer está limitado a IE7 e IE8, y comprueba menos complementos que en otros navegadores.

http://www.itespresso.es/es/news/2010/03/24/mozilla-extiende-herramienta-seguridad-ie-chrome-safari-opera

Más opciones en el Centro de Software

La nueva versión de Ubuntu, Lucid Lynx, traerá entre sus novedades mejoras en el Centro de Software de Ubuntu. De hecho se espera que éste sea uno de los programas que más a fondo se mejorarán en las siguientes versiones de la distribución.
La primera mejora es la aparición de la categoría: "Canonical Partners", que incluirá software de código cerrado disponible en los repositorios y de gran utilidad como puede ser el reproductor de Flash de Adobe.
Aparte, se ha creado una nueva opción de software recomendado que trata de poner algo de orden en una lista tan grande de programas para orientar al usuarios nobel en los programas de mayor popularidad dentro de la comunidad y no perderlo entre programas que quizás no vaya a utilizar nunca.

Deshabilitar notificaciones

Esta noticia la traigo gracias a una entrada que salió en Linux Hispano, blog del que soy uno de sus cuatro administradores, y que redactó Ahornero, uno de los compañeros del sitio web.
Probablemente muchos de vosotros hayáis tenido problemas con las notificaciones que aparecen en la parte superior derecha de la pantalla cuando estéis viendo una película, redactando algo, trabajando... ya que al cubrir parte de la pantalla, cuando salen más de una puede resultar molesto.
La solución es deshabilitarlas. Para ello tenemos dos posibilidades.
Cambiar el nombre del servicio: *sudo mv /usr/share/dbus-/services/org.freedesktop.Notifications.service /usr/share/dbus-/services/org.freedesktop.Notifications.service.disabled*
O eliminar los permisos de ejecución del demonio sudo *chmod -x /usr/lib/notification-daemon/notification-daemon.*

Nouveau, nuevo controlador gráfico

A partir de ahora, Ubuntu incluirá por defecto un controlador gráfico libre llamado Nouveau para las tarjetas gráficas Nvidia. Vendrá incluido por defecto en Lucid Lynx y por ahora sólo soportará gráficos 2D. En un futuro se espera que también soporte 3D y se convierta en una alternativa que cubra todas las posibilidades del controlador de código cerrado, que seguirá estando disponible de forma opcional para quien lo necesite como hasta ahora.



Cambio de estética

Si algo he criticado desde estas líneas con rotundidad era el aspecto de Ubuntu. Un producto necesita un diseño atractivo y moderno, más aún si quiere acercarse a un nicho de mercado que no es de los especialistas. Ésto le ocurría a Ubuntu y gracias al cambio anunciado por Canonical a principio de Marzo de 2010, ya es una realidad.

Un sistema operativo de escritorio orientado a la gran masa de usuarios y no sólo a la élite informática, necesita lo primero "entrar por los ojos". El aspecto de Ubuntu ya era bastante mejor que el de otras muchas distribuciones pero los predominantes tonos marrón oscuro, negro y naranja no le aportaban una estética diferenciada y apropiada para su sector del mercado. El cambio de estética llevado a cabo fue anunciado en prácticamente todos los medios tecnológicos de la red, y la tónica general era positiva con la nueva imagen. Esta difusión en la red certifica el buen estado de popularidad de la distribución que sin lugar a dudas mejorará en cuanto se difunda la nueva imagen de la marca.

Personalmente me resulta mucho más atractiva que la anterior y aunque algunos (entre los que me encuentro) le vemos cierta similitud con la imagen de Mac OS y los productos de *la manzana* en general, es muy original y por primera vez desde que existe Ubuntu define un único color como el propio de la marca, el naranja que se combina con un color secundario, un morado berenjena. El naranja es más claro que en otras ocasiones y resulta muy llamativo al usuario. El berenjena es un tono oscuro lo suficientemente alegre como para ormar parte de los fondos de escritorio.

Los valores que intenta transmitir la nueva imagen de marca según Canonical son (según traduzco del comunicado emitido por Canonical):

Precisión

Canonical distribuye software de gran calidad y lo hace siempre en el tiempo y fecha determinados (sólo hay que ver la precisión con que salen las nuevas versiones). La herencia de Debian implica que los componentes individuales de la plataforma estén claramente definidos y organizados. No hay basura ni excesos en Ubuntu.

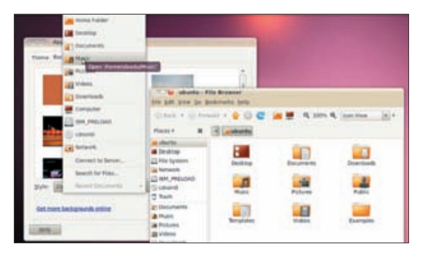
Fiabilidad

Canonical fabrica Ubuntu para un uso serie. Sea cuál sea el uso que le des, si como equipo de escritorio o equipo orientado a trabajar en la nube, se cuida que Ubuntu sea seguro, fiable y predecible. Las actualizaciones que se proporcionan son testadas previamente de forma rigurosa y cuando se comete un error, se toma como punto de partida para que no vuelva a suceder.

Colaboración

Ubuntu es el resultado del trabajo colaborativo entre miles de personas, y que son a la vez los beneficiarios y la cara pública del trabajo de decenas de miles de desarrolladores de software libre. Canonical ha trabajado mucho para que cualquier persona, en cualquier lugar, que esté apasionada por Ubuntu pueda participar. Desde la creación de encuentros físicos, como en el *Ubuntu Develop Summits* a las cuentas de correo pasando por plataformas como Launchpad. Los órganos de decisión de la distribución son un reflejo de todo el trabajo participativo basando a su vez su liderazgo y decisiones, en las decisiones de toda la comunidad que trabaja para la distribución sin cobrar nada a cambio. El cambio, ha afectado a todo lo relacionado con la distribución: el logo, la web, el tema GTK, el fondo de escritorio, el tema que preside Ubuntu Netbook Edition, el *splash*... lo que se dice una reforma integral que le hacía mucha falta al grupo. De hecho ha sido una de las noticias relacionadas con el software libre que más trascendencia han tenido en la red. Desde que se dio a conocer la noticia, todos los portales, blogs y foros relacionados con el software libre en concreto y con la tecnología en general, hablaron y comentaron el nuevo *look*. Sin lugar a dudas una noticia en si mismo el saber que un cambio de estas características ha sido recogido por tantos medios y por lo que he visto, casi todos de forma positiva.

En la red: *https://wiki.ubuntu.com/Brand* – Wiki de Ubuntu.




Intel, el logo de Intel, Intel Core y Core Inside son marcas registradas de Intel Corporation en EE.UU. y el resto de países.

Actualización de Enterprise Server 5
Mandriva ha anunciado la disponibilidad de la actualización de su Mandriva Enterprise Server 5. Con esta actualización los usuarios recibirán una amplia gama de mejoras, incluyendo un aumento significativo de la escalabilidad de virtualización. Mandriva Enterprise Server es un servidor Linux pensado para trabajar en ambientes heterogéneos, con funciones de virtualización, Directorio Activo (basado en OpenLDAP), etc.

Disponible Mandriva 2010 Spring Alpha 3
Ya se encuentra disponible la última versión Alpha de Mandriva 2010 Spring. Posiblemente en abril tendremos a nuestra disposición las dos versiones beta previstas, para tener en junio la RC y en junio la versión final. Podéis encontrar las especificaciones de esta versión en: *http://wiki.mandriva.com/en/uploads/e/e9/Specs2010spring.pdf*

Mandriva en la Solutions Linux trade show
Mandriva estuvo presente en esta feria, celebrada en París del 16 al 18 de marzo. En el stand de Mandriva los visitantes se interesaron especialmente por MandrivaEdu, Mandriva Enterprise Server 5 y Mandriva 2010.0. Por el stand de Mandriva llegaron a pasar más de 500 visitantes.

¿Mandriva la mejor distribución de la década?
En TechSource están realizando la votación sobre la mejor distribución Linux de la década. Tomando como base los rankings de Distrowatch se ha realizado una lista de las 10 mejores distribuciones de la década, en esta lista Mandriva se encuentra en un magnífico segundo lugar. A partir de esta lista se ha animado a los usuarios a votar. En esta votación de usuarios Mandriva está, en este momento, en la PRIMERA posición con un porcentaje de votos del 31%. Enhorabuena Mandriva. Más información en: *http://www.junauza.com/2010/02/best-linux-distributions-of-decade-2000.html*



Blogdrake en Youtube
Dentro de Youtube se ha creado el grupo BlogDrake con la finalidad de que los miembros de la comunidad de Mandriva compartan sus vídeos sobre nuestra distribución GNU/Linux favorita. Podéis encontrar los vídeos en: *http://www.youtube.com/group/blogdrake*

Repositorios de la comunidad

Como ya sabéis los paquetes de software de Mandriva se dividen en tres grandes grupos: Main, que contiene todos los paquetes de software oficialmente soportados; esta fuente no se cambia después de la liberación de distribución al público. Contrib, que contiene paquetes adicionales preparados por colaboradores, estos paquetes tampoco cambian después de la liberación y por último los paquetes Non-free que engloban software con restricciones de licencia y por lo tanto no son libres bajo la GPL. Además de estos grupos oficiales están las fuentes PLF, esto es, paquetes que por diversas causas no pueden incluirse en la distribución. Entre esas causas tenemos: patentes de software, leyes de restricción de la privacidad o leyes de protección de los intereses corporativos. Esta fuente está mantenida por la comunidad.

Además de estos repositorios oficiales tenemos a nuestra disposición otros lugares con software para nuestra Mandriva. En estos lugares encontraremos paquetes que, o bien no podemos encontrar en los repositorios oficiales, o bien han sido compilados con otras opciones. Entre otros tenemos: EduMandriva.ru (*http://edumandriva.ru*), Google (*http://www.google.com/linuxrepositories/urpmi.html*), repositorios de usuarios de Mandriva (*http://mandrivauser.de*, usuarios de Alemania, *http://www.mandrivalinux.gr*, de Grecia o *http://www.mandrivaturkiye.com* de Turquía) y el repositorio de Blogdrake, en el cual nos centraremos. Podéis configurar todos los repositorios de la comunidad de usuarios de Mandriva desde *http://ftp.blogdrake.net/GetRepoDrake*.

Como ya he comentado, y dado que es el repositorio de usuarios de habla hispana, nos vamos a centrar un poco más en el repositorio de Blogdrake. Este repositorio se creó en mayo de 2009 con el objetivo de mantener un repositorio no oficial de Mandriva. En este repositorio se mantienen paquetes que no están incluidos en los repositorios oficiales, o tienen versiones diferentes. Actualmente tienen más de 100 paquetes en sus repositorios.

Además, los empaquetadores mantienen un hilo en Blogdrake donde se aceptan sugerencias de usuarios para crear nuevos paquetes. Lo podéis encontrar en *http://blogdrake.net/consulta/sugiere-crear-un-nuevo-paquete-al-grupo-de-empaquetadores-de-blogdrake*, en este momento el hilo está cerrado por la saturación de trabajo de los empaquetadores, pero en cuanto puedan lo volverán a abrir.

Mandriva con ARM

Mandriva ha anunciado su unión al consorcio ARM Connected Comunity, consorcio que engloba a nada menos que 675 empresas, entre las que se encuentran NVIDIA, OKI y Opera software entre otras (podéis encontrar la lista completa aquí: *http://www.arm.com/community/partners/all_partners.php*). Este consorcio tiene como objetivo la promoción del uso y el soporte de la arquitectura ARM en todo tipo de soluciones.

Pero, ¿qué es la arquitectura ARM? Se llama ARM (Advanced RISC Machines) a una familia de microprocesadores RISC diseñados por la empresa Acorn Computers y desarrollados por Advanced RISC Machines Ltd., que es una empresa derivada de la anterior. Este procesador comparte la filosofía de diseño de los procesadores RISC, es decir, una filosofía de diseño de CPU orientada a un conjunto de instrucciones pequeñas y simples que tienen como ventaja un menor tiempo de ejecución. El diseño del ARM se ha convertido en uno de los más usados del mundo, desde discos duros hasta juguetes. Hoy en día, cerca del 75% de los procesadores de 32 bits poseen este chip en su núcleo.

Puede ser que el nombre del dispositivo o de la tecnología no os suene pero hay multitud de dispositivos móviles que lo llevan en su interior. Por poneros solamente un ejemplo, lo podéis encontrar en la Game Boy Advance, el Iphone o en el novísimo Ipad. La arquitectura ARM se está convirtiendo en la plataforma de referencia para dispositivos móviles.

Aunque no se sabe mucho sobre la aportación de Mandriva a este consorcio, se rumorea que nuestra distribución Linux favorita ofrecerá en algún momento una edición específica de su distribución compatible con este procesador, por lo que quizás en breve podamos utilizar nuestra distribución en un teléfono móvil, una PDA o cualquier otro dispositivo móvil.

Repositorio KDE

Uno de los entornos de escritorio con más solera y con más adeptos es sin duda KDE y por supuesto Fedora no iba a dejar de estar a la última en este aspecto ya que Red Hat siempre ha buscado fomentar su uso mediante su proyecto de KDE.

Para todos aquellos que son usuarios habituales, fanáticos o no, de esta interfaz, éste es un repositorio que no puede faltar. Para ello KDE Red Hat posee tres repositorios:

- Estable: es el más aconsejable para los que quieran estabilidad ya que los paquetes han sido probados durante el tiempo suficiente como para ser usado en lo que se llama ambientes de producción.
- Testing: los que se sientan un poco atrevidos y deseen conocer los últimos paquetes en pruebas en estos repositorios los encontrarán.
- Unstable: es la versión para los audaces y sin miedo a que se rompa su KDE ya que contiene lo más reciente en paquetería, sin probar.

Hay que hacer mención a que los repositorios testing y unstable vienen deshabilitados por defecto ya que su uso para la gran mayoría no es demasiado recomendable.

Si queremos agregar el repositorio KDE a Fedora de Red Hat, abrimos una terminal y nos logueamos como root para después escribir la siguiente orden:

```
$ su -c 'yum -y install wget &&
wget http://apt.kde-redhat.org/apt/
kde-redhat/fedora/kde.repo -O /etc/
yum.repos.d/kde.repo'
```

Con esto ya habremos incluido el repositorio en nuestra lista de fuentes así que ahora lo que toca es actualizar con el siguiente comando en la consola:

```
$ su -c 'yum update'
```

De este modo se descargarán las actualizaciones de los paquetes si es que han sido actualizados.

Rawhide el repositorio de desarrollo de Fedora

Aunque hay quien dice que el desarrollo de Fedora es acelerado en exceso, el trabajo de desarrollo e innovación se produce en los aproximadamente seis meses que hay entre un lanzamiento y el siguiente y una de las herramientas que se utilizan para esta tarea es Rawhide.

El repositorio Rawhide, que es como se conoce al repositorio de desarrollo de Fedora, es donde los desarrolladores depositan las nuevas versiones de los paquetes de software. Se trata de aplicaciones que se actualizan a diario y es realmente vertiginoso el progreso, pero esta rapidez tiene un precio que hay que pagar por ello y es que son paquetes experimentales y sin depurar por lo tanto tendremos errores, incompatibilidades, etc.



Existe desde los comienzos de la distribución, es decir desde la primera versión de Fedora, y el mecanismo es el siguiente: los nuevos paquetes son depositados hasta la versión Alpha de la próxima versión y a partir de aquí ya lo único que se hace es corregir los posibles errores y pulir las aplicaciones.

A partir de esta versión tenemos que el repositorio de desarrollo va a poder almacenar paquetes de hasta dos versiones consecutivas, ya que ha sido ampliado el margen de soporte hasta los nueve meses, lo que dará lugar a una aceleración del proceso de producción y optimizará los recursos.

Para todos los ansiosos que deseen hacer pruebas, pueden agregar el repositorio Rawhide con la siguiente orden en línea de comandos:

```
$ su -c 'yum --enablerepo=rawhide
update'
```

ClearOS

Distribución de origen canadiense que está diseñada para ser servidor de red y puerta de enlace, pensada para pequeñas empresas y entornos distribuidos. Los servicios incluidos son muy fáciles e intuitivos a la hora de ser configurados ya que tiene una interfaz web que lo hace todo más accesible.
Incluye de serie, como se diría de un coche, antivirus, antispam, VPN, filtrado de contenidos, gestor de ancho de banda, además de la certificación SSL y un analizador de registro de la web entre muchos otros módulos disponibles.
Se ofrece como descarga gratuita y además incluye actualizaciones de seguridad también gratuitas para año y medio.
Los Service Packs son liberados cada cierto tiempo y en ellos se incluyen las últimas actualizaciones con sus correspondientes correcciones de errores, pero si se tiene la versión original o un paquete más antiguo, lo único que tenemos que hacer es visitar la página de actualizaciones con WEBconfig y así instalamos todas las que haya disponibles hasta el momento.

Berry Linux 1.01

Originaria de Japón, esta distribución inició su andadura en noviembre de 2004 y ahora nos presenta su versión 1.01 que si no nos fallan las cuentas es la undécima.
Se trata de una distro de las que suelen ser útiles para mostrar las bondades de Linux a los neófitos o en un ambiente educativo cuando nos dedicamos a la docencia y también muy útil en el caso de que por causas ajenas a nuestra voluntad debamos recuperar nuestro sistema.
Berry Linux posee esa cualidad que no debe faltar en un Live CD que es la detección automática del hardware, punto muy importante, ya que si nos tenemos que poner a configurar perderemos el poco y valioso tiempo que podamos tener. Por ejemplo soporta la mayoría de tarjetas gráficas, tarjetas de sonido, dispositivos SCSI, también los USB así como otros múltiples periféricos. Además si disponemos de hardware de red, realizará una configuración automática del mismo mediante DHCP y así podremos conectarnos a Internet sin problemas.
Por otra parte, si lo que queremos es instalarlo en nuestro disco duro podremos hacerlo una vez nos encontremos en el escritorio, mediante el instalador que posee Berry Linux, tan sólo debemos disponer de 1,7 GB de espacio libre.
Como era de esperar, lo que no hace falta decir es que Berry Linux está basada en una de las distribuciones líderes como es RedHat-Fedora.

Informática forense
y software libre

Francisco Lázaro

Instalar Slackware, después de haber conocido distribuciones como Fedora, SuSE o Ubuntu, es como una especie de dejà vú. ¿Qué te voy a contar precisamente a ti, que a finales de los 90 conociste Linux gracias a esta distro -ahora en su versión 13.0? Fuiste de los que la hacían arrancar en modo de emulación con UMSDOS. Instalaste aquella cosa y contra todo pronóstico funcionó. Experimentaste con ella. A golpe de editor configuraste las X y las obligaste a escribir eñes y tildes hackeando librerías del sistema con un parche descargado de Internet.



es@lpmagazine.org

La cosa no combinaba bien con el resto de tu infraestructura (uno de los primeros Pentium recién estrenado, con Windows 98 y disco duro de quinientos megas con la nueva FAT32). Pero por alguna razón no la borraste. Y por fin una tarde diste el paso definitivo: particionar el disco duro y llevar a cabo tu primera instalación nativa de Linux Slackware sobre un sistema de archivos ext2. Ahí comenzó todo: dejaste abierto el camino hacia otras distribuciones con las que durante años has estado tratando de establecer una vida en común –sin demasiado éxito, por cierto-: *RedHat, SuSE, Debian, Mandrake, Fedora, Knoppix, Ubuntu,...*

Slackware permitió que conocieses un mundo distinto al que percibe el extenso rebaño de usuarios que pasta en los plácidos y aburridos campos eliseos de la GUI. Pasaste largas horas con pantallas de texto, seleccionando medios de instalación, configurando idiomas, tarjetas de sonido e interfaces de red, cavilando sobre el significado de todas aquellas explicaciones en inglés sobre librerías, fuentes del kernel y dependencias. Todavía recuerdas, como si hubiera sido esta misma mañana, la primera vez que salió en pantalla tu primer "segmentation fault".

Bien: estamos en el año 2010 y lo acabas de instalar. Tus dedos se mueven ágiles sobre el teclado. Ya has estado aquí. Lo conoces. Se trata del mismo Slackware, pero actualizado tecnológicamente y con rutinas de detección de hardware que nada tienen que envidiar a las de cualquier otra distribución. También posee propiedades que lo convierten en una poderosa herramienta para la investigación informática forense. Pronto iremos a ello.

Una distro histórica

Slackware fue desarrollada por Patrick Volkerding a partir de SLS -una distribución de Soft Landing Systems-. En un principio Patrick quería utilizarla como plataforma de un intérprete de LISP que necesitaba para un proyecto. Poco a poco fue reparando errores de programación y agregando software, un menú de instalación fácil de usar y como novedad principal el concepto de gestión



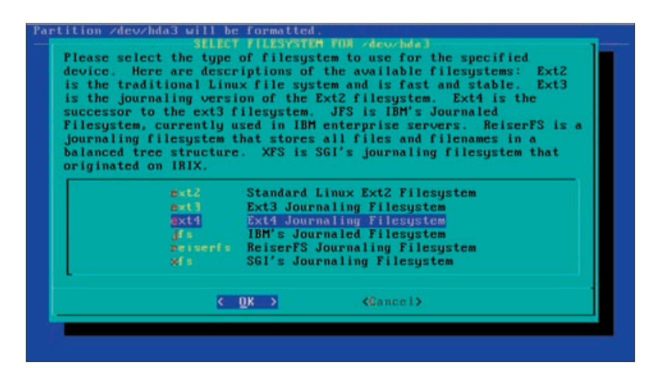


Figura 1. Linux Slackware puede ser asi de espartano...

de paquetes. De estos perfeccionamientos surgió una distribución que no tardó en adquirir popularidad, a la que Volkerding decidió llamar Slackware y poner a disposición de un público más amplio. Corría el año 1993.

Son varias las razones que explican la persistencia de Slackware, pese a todos los avances que han tenido lugar en la escena Linux. Permanece fiel a Unix y no proporciona cómodos interfaces gráficos para las tareas de administración. El usuario tiene un control directo sobre el sistema y puede ver lo que sucede en todo momento. Todavía hoy Slackware goza de una excelente fama como servidor y estación de trabajo para aplicaciones empresariales y de ingeniería.

Slackware está destinado a aquellos usuarios a los que les gusta aprender y disfrutan configurando su sistema para hacer lo que quieren que haga. Por lo dicho, y también por su estabilidad y la simplicidad de su diseño, esta distribución continuará siendo utilizada ampliamente durante los próximos años. Las posibilidades de configuración granular de Slackware permiten construir una estación de trabajo ideal para el informático forense. Pero antes algunos comentarios sobre instalación y estructura del sistema.

Organización del software

No vamos a hablar de cómo conseguir los paquetes y las imágenes de los discos, ni de los diversos métodos de instalación: diskettes –inevitablemente obsoleto-, CD-ROM, DVD, a través de red o directorio NFS; tampoco trataremos sobre requerimientos del sistema, selección del núcleo, diskettes de arranque ni el espartano programa SETUP. El proceso de instalación resulta más sencillo de lo que podría pensarse a la vista de un interfaz basado exclusivamente en pantallas de texto. Todo ello se explica a través de abundante documentación disponible en *www.slackware.com*.

```
PACKAGE SERIES SELECTION
Now it's time to select which general categories of software to install
on your system. Use the spacebar to select or unselect the software
you wish to install. You can use the up and down arrows to see all the
possible choices. Recommended choices have been preselected. Press
the ENTER key when you are finished.

[X] A    Base Linux system
[X] AP   Various Applications that do not need X
[X] D    Program Development (C, C++, Lisp, Perl, etc.)
[X] E    GNU Emacs
[X] F    FAQ lists, HOWTO documentation
[X] K    Linux kernel source
[X] KDE  Qt and the K Desktop Environment for X
[ ] KDEI International language support for KDE
[X] L    System Libraries (needed by KDE, GNOME, X, and more)

< OK >        <Cancel>

The A (base) series contains the kernel and main system utilities.
```

Figura 3. Seleccionando grupos de paquetes

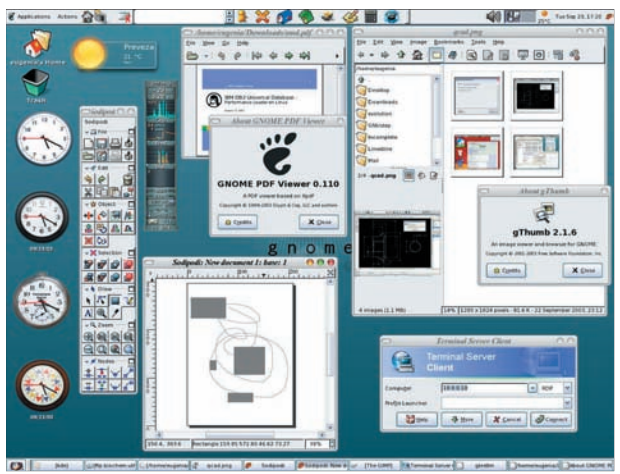


Figura 2. ... o si lo preferimos asi de 'cool'

Slackware estructura su software en paquetes .tgz y un número de utilidades diseñadas para su gestión. Los paquetes aparecen agrupados en varias series:

A	Sistema base, con software para arrancar y hacer funcionar el ordenador, un editor de texto y programas básicos de comunicaciones.
AP	Aplicaciones varias que no requieren X Windows.
D	Herramientas de desarrollo: compiladores, debuggers y ayuda en línea (man).
E	GNU Emacs.
F	Documentación técnica: FAQs, HOWTOs y material sobre temas diversos.
GNOME	Entorno de escritorio del mismo nombre.
K	Código fuente del kernel.
KDE	Entorno de escritorio K, que comparte apariencia y características de diseño con Windows y MacOS. Esta serie incluye también las librerías Q, necesarias para el funcionamiento de KDE.
L	Librerías, incluyendo librerías dinámicas solicitadas por muchos programas.
N	Programas y utilidades para redes, demonios, software de correo electrónico, Telnet, clientes de news, etc.
T	Software TeX para crear documentos científicos.
TCL	TK, TclX, "Tool Command Language".
X	Sistema base X Windows.
XAP	Aplicaciones X no comprendidas en los entornos de escritorio (por ejemplo Ghostscript).
Y	Juegos de consola BSD.

Control granular

Organizar de esta manera el software tiene sus ventajas. A la hora de montar una estación de trabajo, sobre todo cuando no se dispone más que de hardware desfasado, interesa que los recursos estén disponibles para las herramientas: que no haya procesos innecesarios quitando tiempo de procesador a la búsqueda de cadenas de caracteres o al cracking de contraseñas; también queremos que quede en disco la mayor cantidad de espacio –el sistema operativo completo ocupa hasta 6 GB- para guardar imágenes en bitstream, datos del análisis, rainbow tables, etc.

La instalación de Slackware permite elegir no sólo entre grupos de paquetes sino también paquetes concretos dentro de un mismo

grupo (¡ojo con las dependencias!). Aquí lo que nos gustaría es tener las librerías dinámicas, el sistema X Windows y posiblemente también el entorno de desarrollo y las fuentes actualizadas del kernel, por si fuese necesario recompilarlo para incluir alguna característica nueva –soporte para periféricos o sistemas de archivos-. Podemos prescindir por el contrario del supereditor Emacs, de TeX y la serie TCL. También vamos a dejar a un lado GNOME y KDE, grandes consumidores de espacio en disco: los sustituiremos por XFCE, más ligero y económico en recursos.

Slackware permite al investigador seguir una línea recta hasta su objetivo: en vez de instalar un sistema de escritorio completo, para después ir recortando su funcionalidad y aligerándolo de todo aquello que no vaya a hacer falta, conseguimos a la primera un sistema optimizado, tras lo cual no nos quedará más que hacer algunos ajustes para ponerlo en marcha.

Kernel 2.6

La liberación del primer kernel de la serie 2.6.x en diciembre de 2003 supuso un hito en la evolución de Linux. Casi todas las distribuciones actuales se basan en este núcleo. Muchos de los cambios del kernel 2.6.x con respecto a su predecesor 2.4.x responden a criterios de escalabilidad y a la necesidad de utilizar Linux en la empresa. El nuevo kernel incluye modificaciones que atañen al empleo de Linux como plataforma informática forense: para empezar, amplio soporte de dispositivos USB y otros periféricos. Obsérvese que no existe ningún kernel 2.7.x. El paso a la serie 2.6 –última versión estable, en el momento de escribir estas líneas, es la 2.6.33, liberada el 24 de febrero de 2010- supone el abandono del esquema basado en asignar números pares a las versiones estables e impares a las versiones de prueba, supervisadas por los programadores en busca de fallos tras la introducción de nuevas características. La serie 2.5 fue la última en recibir este sistema de numeración. A partir de la 2.6, todos los cambios del kernel son incorporados directamente a la respectiva versión estable 2.6.x.

Lo anterior implica que no cabe excluir la posibilidad de que un cambio en la estructura del kernel provoque fallos catastróficos. No pocos expertos de la comunidad Linux opinan que el kernel 2.6, con su extenso soporte de hardware, constituye un excelente sistema para ordenadores de sobremesa, sin que pueda decirse lo mismo en lo que respecta a servidores y entornos de producción. Aunque esto no lo incapacita para la investigación forense, pueden llegar a necesitarse comprobaciones y una configuración cuidadosa.

El kernel 2.6.x es de uso general y vamos a trabajar con él. La clave de un manejo seguro (y esto vale para todo tipo de software y sistemas operativos) consiste en conocer el entorno y realizar las pruebas adecuadas. No olvidemos algo importante: antes de utilizar sistemas operativos en un entorno profesional de investigación forense, es necesario entender cómo interactúan con el hardware y las aplicaciones.

udev

La gestión de dispositivos constituye un aspecto crucial si se tiene en cuenta que el operario de una estación de trabajo forense estará todo el rato conectando y desconectando discos duros y otros soportes de datos. A partir del kernel 2.6.13 la gestión de dispositivos pasó a ser competencia de un nuevo sistema llamado *udev*. Los nodos -archivos que representan a los dispositivos- utilizados por versiones anteriores del kernel eran estáticos y se hallaban disponibles todo el tiempo en el directorio /dev, hicieran falta o no. Con el nuevo sistema, *udev* crea nodos de dispositivo al vuelo. El directorio /dev se llena en tiempo real a medida que el kernel detecta el hardware durante el arranque.

En Slackware *udev* es un demonio que se ejecuta automáticamente desde el script de arranque /etc/rc.d/rc.udev. El ajuste de nuestra estación de trabajo para fines forenses no obliga a realizar cambios de ningún tipo en este script. *udev* no interviene en el montaje automático de los dispositivos; solamente proporciona un interfaz entre el hardware y el kernel.

Hardware Abstraction Layer

HAL significa "Capa de Abstracción de Hardware". El demonio HAL mantiene en memoria información sobre dispositivos conectados y actúa como intermediario en todo proceso de comunicación con los mismos. Dicha información permanece organizada en un formato coherente accesible a aquellas aplicaciones que quieran acceder a los dispositivos o realizar alguna acción como respuesta a eventos generados por el hardware (conexión, desconexión, etc.). Los datos facilitados por HAL son específicos del objeto y bastante más detallados que los que registra el kernel durante el arranque. De este modo las aplicaciones que reciben desde HAL información sobre un dispositivo pueden reaccionar en el contexto. HAL y *udev* son independientes y no interactúan el uno con el otro. Mientras HAL describe los dispositivos para que las aplicaciones puedan acceder a ellos, *udev* se limita a gestionar nodos de dispositivos. HAL dispone de su propio demonio que arranca mediante el script /etc/rc.d/rc.hald.

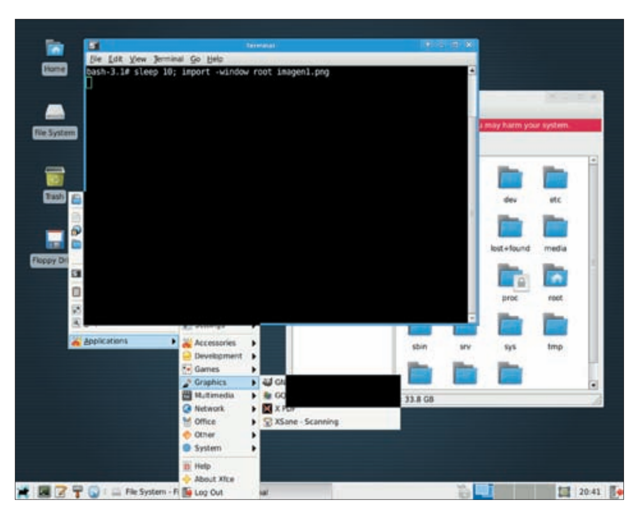


Figura 4. El entorno de escritorio XFCE

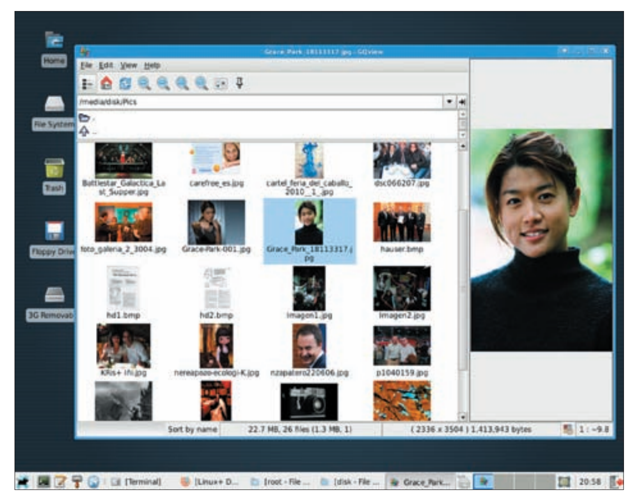


Figura 5. Visualizando imágenes con GQView



Listado 1. Contenido del pendrive mediante 'ls' en la imagen montada

```
root@forensics:~# ls -l

total 87
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 Boda Jenaro
drwxr-xr-x 2 root root 2048 2010-03-02 18:48 docs
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 Elsa Pataky + friends
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 excel
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 Gredos
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 Powerpoint
drwxr-xr-x 2 root root 2048 2010-03-02 18:47 Vdeos Internet
```

Listado 2. Líneas del mensaje encontradas mediante 'grep'

```
root@forensics:~# cat positivos.txt

21982639:
Viene observndose en esta bitcora la actividad habitual de una comentarista que firma bajo el seudnimo
Hypathia. Dicha persona no es la experta en soluciones web interactivas que pretende, sino una simple
agitadora revientaforos al servicio de quien quiera contratarla. Su especialidad consiste en hundir productos
de la industria y la reputacion de profesionales establecidos. Para ello no duda en extender rumores e
historias inventadas, entrar en debates agresivos con otros usuarios, amenazarlos por correo electrnico,
hacer comentarios oscenos, intervenir en los debates con otros nicks, a veces hacindose de palmera a misma,
otras atacndose grosermente para destacar sus puntos de vista y atraer partidarios que la defiendan.En todas
sus intervenciones despliega una tremenda agresividad, habiendo protagonizado casos de acoso moral en ms
.........................................................................
.........................................................................
.........................................................................
```

d-bus

El bus de mensajes del sistema facilita un mecanismo que permite a las aplicaciones comunicarse e intercambiar información. Para simplificar, diremos que *d-bus* es el canal utilizado por HAL para enviar sus datos a las aplicaciones. En Slackware, *d-bus* también arranca como demonio desde /etc/rc.d/rc.messagebus.

Deshabilitando HAL y d-bus

Quienes adquirieron práctica con el montaje manual de dispositivos probablemente se hayan preguntado cómo se las arregla Linux para detectar un lápiz USB en el momento de insertarlo, mostrando un mensaje con botones que permiten abrir un navegador de archivos, reproducir medios u otras opciones. Pues bien: son HAL y *d-bus* quienes hacen posible este fenómeno al mejor estilo Microsoft Windows.

Sin embargo un comportamiento tan amistoso no resulta conveniente en una estación de trabajo para cometidos de investigación. Somos informáticos forenses con un alto nivel de profesionalidad y buenas prácticas, no simples mirones de datos: tenemos que impedir que el medio se vea alterado mediante un montaje accidental del dispositivo. Si no, adiós prueba. La parte contraria se frotará las manos. ¿Cómo le explicaríamos al juez que la diferencia en los hashes de autentificación de un medio en dos momentos sucesivos se debe

Listado 3. Volcado hexadecimal del mensaje injurioso (en parte)

```
root@forensics:~# xxd -s 21981039 pendrive.dd | less

(Texto suprimido)..............................
...............................................
14f92cf: 0054 6520 7661 7320 6120 656e 7465 7261  .Te vas a entera
14f92df: 7200 0000 001e 0000 0024 0000 0043 6f6e  r........$...Con
14f92ef: 7370 6972 6163 696f 6e65 7320 7920 6a75  spiraciones y ju
14f92ff: 6761 7272 6574 6173 2076 6172 6961 7300  garretas varias.
14f930f: 001e 0000 0010 0000 0041 6c6f 6e73 6f20  .........Alonso
14f931f: 5572 7275 7469 6100 001e 0000 0004 0000  Urrutia.........
14f932f: 0000 0000 001e 0000 006c 0000 0053 6520  .........l...Se
14f933f: 7661 2061 2065 6e74 6572 6172 206d 6920  va a enterar mi
14f934f: 6a65 6661 2064 6520 6c6f 2071 7565 2076  jefa de lo que v
14f935f: 616c 6520 756e 2070 6569 6e65 2e20 4e6f  ale un peine. No
14f936f: 206c 6520 6461 72e1 6e20 756e 2070 6564   le dar.n un ped
14f937f: 6964 6f20 6e75 6576 6f20 656e 206c 6f20  ido nuevo en lo
14f938f: 7175 6520 6c65 2071 7565 6461 2064 6520  que le queda de
14f939f: 7669 6461 2e00 0000 001e 0000 000c 0000  vida...........
14f93af: 004e 6f72 6d61 6c2e 646f 7400 001e 0000  .Normal.dot.....
14f93bf: 0004 0000 0020 0000 001e 0000 0004 0000  ..... .........
14f93cf: 0035 0000 001e 0000 0018 0000 004d 6963  .5..........Mic
14f93df: 726f 736f 6674 204f 6666 6963 6520 576f  rosoft Office Wo
14f93ef: 7264 0000 0040 0000 0000 180d 8f00 0000  rd...@.........
14f93ff: 0040 0000 0000 dca3 cffc b9ca 0140 0000  .@..........@..
(Texto suprimido)..............................
...............................................
14fa29f: 001e 0000 0048 0000 0049 4e44 5245 2028  .....H...INDRE (
14fa2af: 496e 6475 7374 7269 6120 4e61 6369 6f6e  Industria Nacion
14fa2bf: 616c 2070 6172 6120 6c61 2044 6566 656e  al para la Defen
14fa2cf: 7361 2064 6520 6c6f 7320 5265 6375 7273  sa de los Recurs
14fa2df: 6f73 2064 6520 4573 7061 f161 2900 0000  os de Espa.a)...
14fa2ef: 0003 0000 000c 0000 0003 0000 0003 0000  ...............
14fa2ff: 0003 0000 0026 0700 0003 0000 00e6 150b  .....&.........
14fa30f: 000b 0000 0000 0000 000b 0000 0000 0000  ...............
14fa31f: 000b 0000 0000 0000 000b 0000 0000 0000  ...............
14fa32f: 001e 1000 0001 0000 0011 0000 0054 6520  ............Te
14fa33f: 7661 7320 6120 656e 7465 7261 7200 0c10  vas a enterar...
14fa34f: 0000 0200 0000 1e00 0000 0700 0000 54ed  .............T.
14fa35f: 7475 6c6f 0003 0000 0001 0000 0000 0000  tulo...........
14fa36f: 0000 0000 0000 0000 0000 0000 0000 0000  ...............
...............................................
...............................................
```





Figura 6. Navegando por Internet con Firefox bajo XFCE

al cambio de unos pocos bytes, y no de una manipulación dolosa o cuando menos incompetente como alega la parte contraria?

En dicho contexto el automatismo de HAL y d-bus resulta embarazoso y nos vemos obligados a desconectarlo. Queremos que el sistema haga lo que le digamos, no lo que él considere bueno para el usuario. Buenas noticias: los cambios son fácilmente reversibles, y el lector podrá seguir beneficiándose de la inversión de esfuerzo y tiempo realizada hace años mientras adquiría soltura con la compleja sintaxis del comando *mount*.

Permisos de ejecución

Aunque en Slackware la organización de los scripts de arranque sigue el esquema de BSD, a partir de la versión 7.0 se introdujo un modo de compatibilidad con System V, existiendo un directorio por cada nivel de ejecución -de 0 (apagado) a 6 (reinicio del sistema), pasando por 1 (modo simple monousuario), 2, 3 y 5 (normal, red y X, todos ellos multiusuario), y finalmente 4 (sin asignar)- con los scripts correspondientes (guiones o listas de comandos que ejecutan una serie de tareas automatizadas, de modo similar a los primitivos archivos de MS-DOS AUTOEXEC.BAT y CONFIG.SYS). Una vez establecido el *runlevel* mediante inittab y ejecutados los scripts generales de arranque, responsables de tareas como inicialización del sistema, montaje de los sistemas de archivo y otras funciones, correrá el script por defecto de Slackware: /etc/rc.d/rc.M, cuyo cometido consiste en



Figura 7. Evidencia hallada entre las pertenencias del sospechoso

iniciar diversos demonios y servicios del sistema. Si examinamos este script:

```
root@forensics:~# cat /etc/rc.d/rc.M
```

podremos comprobar que contiene varias líneas de este estilo:

```
...
if [ -x /etc/rc.d/rc.pcmcia ]; then
   . /etc/rc.d/rc.pcmcia start
...
```

La sentencia condicional indica que el script sólo será invocado desde rc.M si dispone de permisos de ejecución. Puesto que trabajamos con un kernel 2.6 y queremos evitar que nuestra estación de trabajo forense acceda a los soportes de datos sin autorización del usuario, lo único que tenemos que hacer es cambiar los permisos de ejecución de los scripts que inician HAL y d-messagebus durante el arranque del sistema:

```
root@forensics:~# chmod 644 /etc/rc.d/rc.hald
root@forensics:~# chmod 644 /etc/rc.d/rc.messagebus
```

Esto no impide que los dispositivos sean detectados por el kernel: tan solo evita el montaje automático de los mismos. Los cambios serán efectivos tras un reinicio del sistema.

Herramientas

Disponemos ya de una plataforma informática forense que cumple todos los requisitos para una investigación profesional. Sobre ella instalaremos nuestras herramientas forenses: *Sleuthkit+Autopsy*, recuperadores de particiones y archivos borrados como *Testdisk* y *Photorec*, herramientas para tallado de archivos ("*data carving*") como *Foremost* y *Scalpel*, utilidades y scripts de Perl para la búsqueda de cadenas de caracteres y el análisis de correo electrónico, cookies, etc.

Linux incluye un número de utilidades que convierten a Slackware en una distribución ideal para la investigación forense. He aquí algunas:

- dd: la "navaja" suiza del mundo Linux, para copiar y manipular fragmentos de archivos a bajo nivel, obtener imágenes en bitstream y duplicar todo tipo de soportes de datos.
- sfdisk y fdisk: con ellos podremos determinar la estructura y particiones de un disco duro.
- grep: búsqueda de cadenas de caracteres o expresiones regulares en archivos.
- dispositivo loop: para asociar archivos convencionales con nodos de dispositivo, muy útiles a la hora de montar una imagen en bitstream sin tener que trasladarla antes a un disco duro o DVD.
- md5sum y sha1sum: creación y almacenamiento de hashes de autentificación forense para archivos y dispositivos.
- file: lee la información de cabecera de un archivo y determina el tipo del mismo independientemente de su nombre o extensión.
- xxd: editor hexadecimal en línea de comando, para examinar el código en bruto de un archivo.

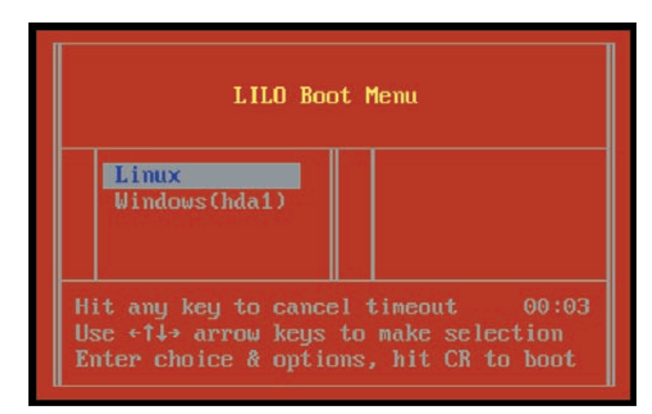


Figura 8. Slackware utiliza LILO como gestor de arranque

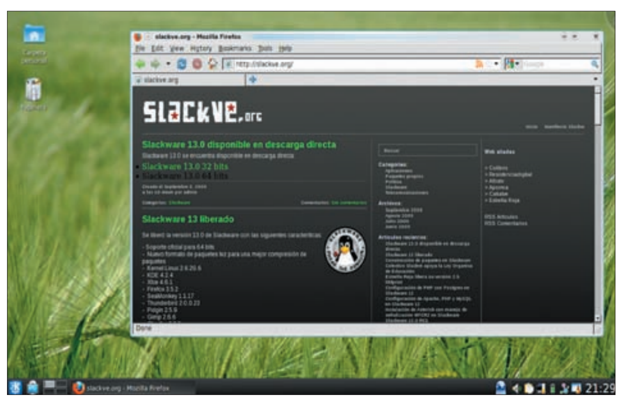
No quiero acabar este apartado sin mencionar el nombre de Barry J. Grundy, investigador especial del gobierno de Estados Unidos y autor de un extenso documento sobre Informática Forense con Linux que me ha aclarado las dudas técnicas referentes a los automatismos del arranque, y que figura citado en la lista de enlaces al final de este artículo. Tampoco dejes de consultar las páginas man. Para algo ha de servir que las incluyan en todas las distros. Asimismo hallarás una valiosa ayuda en Internet. En respuesta a tu última duda, ahora que estás frente a la GUI, pensando que tal vez no haya sido tan buen negocio cambiar GNOME por XFCE: no te preocupes, también se puede escribir en el idioma de Cervantes. Abre una consola y teclea esto: *user@forensics:~$ setxkbmap es*.

Caso práctico: pánico en el Consejo de Administración

Si el lector ha tenido paciencia para seguir hasta aquí es justo recompensarle con algo más ameno: un ejemplo de aplicación de los conocimientos adquiridos. Los hechos son ficticios, pero posiblemente todos los días suceden cosas peores sin que se llegue a saber cuál es la mano negra que mece la cuna de nuestro infortunio. Hoy es diferente, pues el destino quiere que haya cerca un informático forense para hacer justicia: tú.

Desde hace meses trabajas en una importante casa del sector aeroespacial. Tu jefa necesita ayuda: en varios foros de la industria de Defensa están publicando un copypaste injurioso en el que se la acusa de ser autora de determinados comentarios provocadores y xenófobos. En un retorcido alarde de bajeza, el autor de la intoxicación, quien posiblemente haya escrito también con anterioridad los comentarios racistas a los que la misma se refiere (referentes a directivos y trabajadores en prácticas del grupo empresarial), escribe cosas como esta:

"Con el propósito de no dejar impunes los actos viles y cobardes de la susodicha elementa, tenemos a bien informar de que su verdadero nombre es ********* ********* ******, con domcilio en el ** de la calle ********, 28001 Madrid. Su teléfono móvil es el: ***


Figura 9. Slackware y KDE: vastas praderas hasta donde alcanza la vista, pero no es Windows... Afortunadamente



*** ***. Trabaja como conserje en ***** y dedica la mayor parte de su tiempo laboral a llevar a cabo estos actos desde la misma red de la empresa, actvidad por la que ha sido reconvenida en varias ocasiones por la dirección."

¿Alguna pista? La joven ejecutiva sospecha de Urrutia, el trompo más holgazán e intrigante de la oficina, que trabaja en Gestión de Pedidos. No solo porque a raíz de este mensaje acaba de recordar que una vez tuvo que hacer algo con el ordenador de su departamento y comprobó que no escribía bien las íes, sino también por lo irónico de la jugarreta. Hace un mes tu jefa reprendió al empleado tras haberle sorprendido en su matarratos favorito: distribuir vídeos de primera y powerpoints con chistes sexistas a través del correo electrónico de la empresa.

Urrutia es un hombre vengativo y desde entonces ha estado tramando su desquite: no tolera verse humillado por una mujer joven, guapa, con talento y mejor preparada que él. Los mismos motivos que tiene él para odiar a tu jefa tú los tienes para acudir al rescate. Los indicios disponibles no bastan para acusarle. Necesitáis pruebas sólidas, así que con la ayuda del vigilante jurado, y aprovechando que es el día libre de ese personajete, entráis en su despacho para practicar un discreto registro.

Urrutia sabe algo sobre direcciones IP y logs y no se habrá arriesgado a llevar a cabo su fechoría desde el trabajo, sino que lo habrá hecho desde su casa o habrá ido a un cibercafé. Tampoco encontrarás pruebas en su ordenador. Por si fuera poco, todos los días, a la hora de comer, se ejecuta automáticamente el desfragmentador de disco, con lo cual existe una alta probabilidad de que toda evidencia residual haya sido destruida.

Imagen en bitstream

Estás de suerte. En el cajón de su escritorio halláis un antiguo pendrive de 256 MB. Te lo llevas a casa, tras haber prometido a tu jefa que harás todo lo que puedas, y nada más llegar te pones a ello. Como buen informático forense sabes que no conviene trabajar sobre el soporte, así que lo primero que haces es arrancar Slackware 13.0 y realizar una imagen a bajo nivel con el comando dd, antes de dejar la llave USB en el interior de una bolsita de plástico precintada:

```
root@forensics:~# dd if=/dev/sda1
    of=pendrive.dd
```

Ese archivo denominado pendrive.dd contiene todo lo que hay en la llave USB, y además los archivos borrados y todo el espacio no asignado por el sistema de archivos, incluyendo el slack (datos residuales comprendidos entre el final de los datos guardados y el final del sector y del cluster donde se halla el último fragmento del archivo) y datos previos a un reformateo del soporte.

El cacheo

Acto seguido montas la imagen con el dispositivo loop y examinas su contenido:

```
root@forensics:~# mkdir zzzz
root@forensics:~# mount -o loop pendrive.dd zzzz
root@forensics:~# cd zzzz
root@forensics:~# ls -l
```

Examinas los resultados (Listado 1). En la imagen hay varias carpetas con un total de 87 documentos. “Vdeos Internet” y “Powerpoint”, como era de esperar, incluyen los resultados del último remoloneo de nuestro amigo Urrutia por cosasgraciosas-punto-com. “Boda Jenaro” contiene fotografías tomadas durante los esponsales de un compañero del trabajo, y “Gredos” imágenes del chalet que el sospechoso está construyendo en la sierra. Sin comentarios en cuanto al contenido de la carpeta “Elsa Pataky + friends”.

Más interesantes parecen las carpetas “EXCEL” y “DOCS”. Tras examinarlas descubres algunas hojas de cálculo con listas de precios y correspondencia comercial: modelos de oferta, una admonición por retrasos en los pagos y dos o tres respuestas a reclamaciones de clientes.

Búsqueda de caracteres con *grep*

No has conseguido gran cosa: una muestra de cultura popular en Internet y una colección de actrices y tenistas ligeras de ropa. Llegó la hora de bucear en el espacio no asignado en busca de evidencia oculta. Sabes lo que buscas y esto es una ventaja porque te permite desplegar todo el poderío de grep, ese Hércules de la mitología Linux. Editas un archivo con algunos de los términos que aparecen en el anónimo, como “agitadora”, “cobardes”, “conserje”, “elementa”, etc., y lo pasas como parámetro al comando de búsqueda más célebre de todos los tiempos.

```
root@forensics:~# grep -abif lista.txt pendrive.dd >
positivos.txt
```

La opción a ordena a grep que procese nuestra imagen como archivo de texto sin tener en cuenta los caracteres binarios; b introduce el número (decimal) de posición donde aparece cada una de las coincidencias; i desactiva la distinción entre mayúsculas y minúsculas, y f sirve para indicar que la búsqueda se realiza en un archivo y no en el disco duro.

Tus desvelos se ven coronados por el éxito, y muy pronto puedes ver en pantalla el escrito injurioso (véase comienzo del mismo en el Listado 2). Tras examinarlo minuciosamente con el visor hexadecimal xxd, después de desplazarte hasta el número de línea que figura al comienzo del archivo “positivos.txt”, compruebas que se trata de un documento MS-Word. No figura en ninguna carpeta porque que el sospechoso lo borró. Por si quedaran dudas, los metadatos del archivo se encargan de disiparlas (Listado 3).

Recuperación del archivo borrado

Misión cumplida: has encontrado el cuerpo del delito. Sin embargo, se te ocurre que sería mejor llevar a tu jefa no un volcado hexadecimal, sino el propio documento visto a través de MS-Word o StarOffice. Para extraer el archivo borrado puedes utilizar varias estrategias: por ejemplo servirte de las herramientas del sistema para localizar el principio del documento mediante una búsqueda de sus caracteres “mágicos” (en el caso de los documentos Word, la cadena hexadecimal “d0cf 11e0 a1b1 1ae1” más próxima antes de llegar a la posición localizada por grep), luego el final (algo después de la etiqueta que indica la versión de Word con que fue creado el documento, incluyendo algunas líneas adicionales, que Office ignorará, eliminándolas al guardar de nuevo), para terminar recortando con dd todo el código comprendido entre ambos puntos.

Otra opción consiste en desenterrar el archivo con icat (comando perteneciente a la suite SleuthKit), pero no te servirá de nada si el medio ha sido reformateado. Finalmente puedes hacer un barrido de todo el soporte con Foremost o Scalpel. Esto sería como zarandear el olivo con la red en tierra, y nos permitiría averiguar con qué otros archivos puede haber estado trabajando -o en su caso perdiendo el tiempo- el villano de nuestra historia.

Conclusiones: potencial de Linux como herramienta de investigación forense

Slackware no es la única distribución para investigadores, pero sí una de las que se adapta con mayor facilidad a la práctica profesional en condiciones de higiene forense, sin montaje automático de sistemas de archivos y sin interferencia imprevista de aplicaciones o servicios del sistema. Permite trabajar con el sabor más tradicional de Unix y proporciona control granular sobre la configuración del sistema. En Slackware la instalación de herramientas todavía se lleva a cabo al modo antiguo, bajando el paquete .tgz de la página del desarrollador y sometiéndolo al proceso habitual de descompresión, compilación e instalación. Por cierto: aun te acuerdas de todo aquel ritual de tar -xfzv, make, etc., ¿verdad?

En nuestros días la investigación forense no se hace así. Policía, detectives privados y responsables de seguridad de las grandes empresas trabajan con suites tipo EnCase Forensics y FTK, duplicadores de discos y dispositivos de bloqueo de escritura. Todo ello bajo Windows, con un amplio y caro apoyo logístico de formadores y soporte técnico. No tengo mucha noticia de cómo le va al gremio en estos tiempos, pero es de suponer que pese a tratarse de un sector en expansión tampoco habrá podido sustraerse a los rigores de la crisis. Linux permitiría lograr un ahorro de costes importante, sobre todo en la administración pública.

La clave para que Linux y el código libre prosperen reside en lograr un equilibrio satisfactorio entre facilidad de uso, excelencia técnica y coste de la formación. El valor didáctico de Linux, concretamente de distribuciones como Slackware, es evidente. En el mundo de las tecnologías de la información podría compararse al sistema del pingüino con uno de esos literatos que no escriben para las masas, sino para otros escritores. Linux no es para usuarios que ocasionalmente se ven obligados a realizar tareas de investigación en busca de archivos pedófilos, bases de datos robadas o pruebas de mala conducta que permitan incriminar al Urrutia de turno. Linux está hecho para los propios investigadores, para enseñarles cómo funciona a bajo nivel el software, nutrir su vocación profesional y ponerlos en situación de dar ante un juez explicaciones relativas a los aspectos más intrincados de la tecnología informática forense.



En la red

- *http://www.slackware.com/*
- *http://www.slackware-es.com/*
- *http://www.linuxleo.com/*
- *http://news.cnet.com/Linux-tool-speeds-up-computer-forensics-for-cops/2100-7344_3-6233311.html*
- *http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-willis-c/bh-us-03-willis.pdf*
- *http://www.bilbos-stekkie.com/slack_init/en/index.htm*

Hachoir:
Framework para manipular archivos binarios

Alonso Eduardo Caballero Quezada

Cuando se realiza análisis forense, una de las fases en la metodología forense, es inherente trabajar con archivos binarios. *Hachoir* es la palabra francesa utilizada para un picador de carne, el cual es utilizado por los carniceros para dividir la carne en secciones largas. *Hachoir* es utilizado por los carniceros en cómputo forense para dividir los archivos binarios en campos. De esta manera permite visualizar y editar campo por campo flujos binarios o secuencias binarias.



es@lpmagazine.org

En otras palabras permite "navegar" cualquier flujo binario como si se navegaran directorios y archivos, de esta manera un archivo se divide en un árbol de campos, donde el campo más pequeño es de solamente un bit. También existen otros tipos de campos, como por ejemplo: enteros, cadenas, bits, tipos relleno, flotantes, etc. El presente artículo presenta *Hachoir* en su aspecto teórico, acompañado de algunos ejemplos prácticos. Hachoir es un framework para manipular archivos binarios escrito en Python, el cual es independiente del sistema operativo y tiene más de una interfaz de usuario en modo texto y gráfico (ncurses, wxWidget, Gtk+). Aunque Hachoir también permite editar archivos (de los formatos soportados), sin el programa original (algunas veces propietario) que fue utilizado para crearlo, generalmente está orientado a examinar archivos existentes. Actualmente Hachoir soporta más de sesenta formatos de archivo. El reconocimiento está basado en las cabeceras y pies en una imagen de disco o archivo. Se tiene un intérprete que es tolerante a fallos diseñado para manejar archivos truncados o con errores. El framework también ajusta automáticamente temas como el juego de caracteres y endian. También puede ser extendido y utilizado con scripts.

Hachoir está compuesto de un núcleo que es el encargado de realizar el análisis (*Hachoir-core*). El paquete incluye algunos programas de ejemplo basados en el núcleo del *framework* y el analizador:

- *hachoir-parser*: analizador de varios formatos de archivos y otros programas periféricos.
- *hachoir-metadata*: extrae los metadatos. Por ejemplo, puede ser utilizado para extraer información de fotos y vídeos favoritos.
- *hachoir-strip*: retira los metadatos y otra información "inútil".
- *hachoir-grep*: ubica subcadenas en un archivo binario (utilizando los analizadores de Hachoir: así la búsqueda es sensible a *Unicode*).
- *hachoir-subfile*: encuentra todos los sub archivos en un archivo.

Instalación

Se puede realizar la instalación de *Hachoir* utilizando los paquetes disponibles para Debian, Mandriva, Gentoo, Arch y FreeBSD.

También es factible realizar la instalación de *Hachoir* desde su código fuente, para esto se tiene que proceder a descargar todos los *tarballs* pertinentes. La instalación debe proceder de una manera ordenada y secuencial, para que no se presenten inconvenientes en lo que respecta a las dependencias. Cada *tarball* debe ser descomprimido, para luego proceder a ingresar al directorio creado por esta acción, luego de lo cual se debe proceder a ejecutar el archivo *setup.py*, de la siguiente manera:

```
# python setup.py install
```

Si no se tuvieran los privilegios de administrador, también es posible proceder con la instalación, siguiendo las instrucciones antes descritas, pero en lugar de ejecutar *python.py*, se debe utilizar:

```
$ DIR=$HOME/hachoir
$ ./setup.py install --install-script=$DIR --install-
purelib=$DIR
```

Finalmente la más reciente versión de *Hachoir* siempre está en *Mercurial,* que es un sistema de gestión de versión de fuente rápido y liviano diseñado para manejar de manera eficiente una cantidad muy grande de proyectos distribuidos. La instalación de Hachoir utilizando *Mercurial* es similar a la instalación desde el código fuente. Pero en lugar de descargar los *tarballs* se utiliza el siguiente comando:

```
# hg clone http://bitbucket.org/haypo/hachoir/
```

Se debe utilizar *source setupenv.sh* para configurar la variable de entorno *PYTHONPATH* (para que *Hachoir* lo utilice dentro de la instalación).

La Figura 1 muestra el resultado de aplicar el comando antes detallado y la estructura de directorios y archivos que ha creado *Mercurial*, con lo cual se puede proceder a instalar *Hachoir* desde las fuentes.

Para propósitos del presente artículo se ha procedido a instalar *Hachoir* desde los repositorios existentes para Ubuntu. En la Figura 2 se muestra el listado y el inicio del proceso de instalación de estos paquetes.

A continuación se procede a detallar los programas, módulos y programas experimentales más relevantes de Hachoir.

hachoir-core

Es el núcleo de *Hachoir*, las características más importantes son las siguientes: autofix (arreglo automático): en caso de error, *Hachoir* puede arreglar de manera automática los errores de archivos con fallas o del intérprete. *Hachoir* es capaz de arreglar (algunos) errores del intérprete; errores desde archivos de entrada no válidas, truncadas o desde el código del intérprete.

- Si un campo es mayor de lo que debería ser, es removido o truncado.
- En un error del intérprete, el campo es removido.
- Cuando la interpretación se ha realizado, de ser necesario el conjunto de campos se completa con relleno.

Perezoso (lazy): los campos como el valor, tamaño, descripción, direcciones absolutas, etc., son calculados bajo demanda.

Se han retirado todas las características de *Hachoir* que puedan resultar perezosas: esto significa que *Hachoir* lee y calcula una información sólo cuando se le requiere o si *Hachoir* lo necesita para leer o calcular otra información. Ejemplos:

- Los valores y descripciones del campo se leen y crean en el primer acceso.
- Los campos de un conjunto de campos son creados bajo demanda, o si *Hachoir* no es capaz de adivinar el tamaño del conjunto de campos, etc.

Debido a la característica *Lazy* (perezoso), *Hachoir* es capaz de leer archivos de gran tamaño como una partición FAT de 10GB y crear un árbol de campos profundo y complejo. El secreto es la palabra clave *yield* en Python.

- Sin límite arbitrario: *Hachoir* no tiene un límite arbitrario. Las direcciones pueden ser más grandes que 4G, un entero puede ser de 32, 64, 128 bits o más, no hay un límite de número de campo, límite de profundidad, etc.
- Tipos: *Hachoir* tiene varios tipos de campos predefinidos: entero, cadena, boolean, cadena de bytes, etc.
- Granularidad de bit: los tamaños y direcciones están en bits, así que es fácil fusionar campos con tamaño en bytes o en bits.
- Unicode: los valores de una cadena son almacenados en Unicode (si se especifica el juego de caracteres).
- Endian: no es necesario preocuparse sobre *endian,* sólo es necesario configurarlo una sola vez para el intérprete.
- Sin dependencia: *Hachoir* solamente necesita Python 2.4 (pero algunas delanteras necesitan más librerías).

```
root@reydes:/media/hda3/tools/forensics# hg clone http://bitbucket.org/haypo/hac
hoir/
destination directory: hachoir
requesting all changes
adding changesets
adding manifests
adding file changes
added 1206 changesets with 2781 changes to 413 files
updating working directory
357 files updated, 0 files merged, 0 files removed, 0 files unresolved
root@reydes:/media/hda3/tools/forensics/hachoir# ls
benchmark.sh      hachoir-gtk       hachoir-subfile  snapshot.sh
coverage_test.py  hachoir-http      hachoir-tools    test_code.sh
coverage_test.sh  hachoir-metadata  hachoir-urwid    test_code_snapshot.sh
hachoir-core      hachoir-parser    hachoir-wx
hachoir-editor    hachoir-regex     setupenv.sh
root@reydes:/media/hda3/tools/forensics/hachoir#
```

Figura 1. Resultado de utilizar el comando *hg clone* para proceder a instalar *Hachoir*

```
root@reydes:~# apt-cache search hachoir
python-hachoir-core - Core of Hachoir framework: parse and edit binary files
python-hachoir-metadata - Program to extract metadata using Hachoir library
python-hachoir-parser - Package of Hachoir parsers used to open binary files
python-hachoir-regex - regular expressions manipulation Python library
python-hachoir-subfile - find subfiles in any binary stream
python-hachoir-urwid - Binary file explorer using Hachoir and urwid libraries
python-hachoir-wx - wxWidgets GUI for the hachoir binary parser
root@reydes:~# apt-get install python-hachoir-core
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalaron de forma automática los siguientes paquetes y ya no son necesarios
.
  freetds-common libotr2 liblog4j1.2-java snmp libgdchart-gd2-noxpm libct4
  libgcj9-0-awt libmx4j-java
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
  python-profiler
Paquetes sugeridos:
  python-hachoir-parser python-hachoir-urwid python-hachoir-metadata
  python-doc
Se instalarán los siguientes paquetes NUEVOS:
  python-hachoir-core python-profiler
```

Figura 2. Listado de paquetes en los repositorios e inicio de la instalación en Ubuntu

```
255 cabezas, 63 sectores/pista, 0 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Identificador de disco: 0x2a006733

Disposit. Inicio    Comienzo      Fin      Bloques  Id  Sistema
hdb.dd1   *            1          401      3221001   7  HPFS/NTFS
hdb.dd2              402          784      3076447+  f  W95 Ext'd (LBA)
hdb.dd5              402          784      3076416   b  W95 FAT32
root@reydes:/media/hda3# cat hdb.md5
7a31655a4d6381744d6efb2f9205bb9a  hdb.dd
root@reydes:/media/hda3# mmls hdb.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0006442064   0006442002   NTFS (0x07)
03:  Meta    0006442065   0012594959   0006152895   Win95 Extended (0x0F)
04:  Meta    0006442065   0006442065   0000000001   Extended Table (#1)
05:  -----   0006442065   0006442127   0000000063   Unallocated
06:  01:00   0006442128   0012594959   0006152832   Win95 FAT32 (0x0B)
root@reydes:/media/hda3#
```

Figura 3. Estructura de las particiones y los sistemas de archivos del archivo *hdb.dd*

- API: los datos son representados como un árbol de campos donde cada campo es un objeto en Python.

Un archivo es dividido en un árbol de campos. Un conjunto de campos es también un campo, y cada campo es un objeto. Algunos atributos interesantes son:

- *size*: tamaño en bits,
- *value*: valor del campo,
- *description*: cadena de descripción,
- *address*: dirección relativa (relativa a la dirección padre absoluta),
- absolute_address: dirección en un flujo,
- *Intérprete*: se incluyen 70 intérpretes: imágenes JPEG, archivos ZIP, audio MP3, y muchos más,
- *Intérprete de aproximación* (*Guess parser*): un algoritmo que selecciona de manera automática el intérprete correcto utilizando la extensión del archivo, considerando el tipo MIME, o usando la función *validate()* de cada intérprete,
- *Editor*: utilizando la representación de datos de *Hachoir*, se puede editar, insertar, retirar datos y guardarlos en un nuevo archivo.

hachoir-metadata

hachoir-metadata es una herramienta para extraer los metadatos de archivos multimedia (sonido, vídeo, etc.), pero también archivos, y soporta los formatos de archivos más comunes.

Hachoir-metadata intenta proporcionar tanta información como sea posible. Por ejemplo para algunos formatos de archivo proporciona más información que *libextractor. GNU libextractor* es una librería utilizada para extraer metadatos de archivos de tipo arbitrario, tal como el intérprete RIFF, el cual puede extraer la fecha de creación, software utilizado para generar el archivo, etc. Pero *hachoir-metadata* no puede adivinar la información. La operación más compleja es

```
     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0006442064   0006442002   NTFS (0x07)
03:  Meta    0006442065   0012594959   0006152895   Win95 Extended (0x0F)
04:  Meta    0006442065   0006442065   0000000001   Extended Table (#1)
05:  -----   0006442065   0006442127   0000000063   Unallocated
06:  01:00   0006442128   0012594959   0006152832   Win95 FAT32 (0x0B)
root@reydes:/media/hda3# mount -o ro,loop,offset=32256 -t auto hdb.dd s_hdb1/
root@reydes:/media/hda3# mount -o ro,loop,offset=3298369536 -t auto hdb.dd s_hdb
5/
root@reydes:/media/hda3# ls s_hdb1/
Archivos de programa     Downloads      ntldr                     t144
AUTOEXEC.BAT             fvnja6hw.sys   pagefile.sys              t2q4
Bootfont.bin             imagen.nrg     Progra~1                  Thumbs.db
boot.ini                 IO.SYS         RECYCLER                  $VAULT$.AVG
Config.Msi               mIRC           sqmdata00.sqm             WINDOWS
CONFIG.SYS               MSDOS.SYS      sqmnoopt00.sqm            YServer.txt
Documents and Settings   NTDETECT.COM   System Volume Information
root@reydes:/media/hda3# ls s_hdb5/
Archivos de programa     recycled                      UnicodeRelease
Config.Msi               System Volume Information
Documents and Settings   temporal
root@reydes:/media/hda3#
```

Figura 4. Montaje de las dos particiones contenidas en *hdb.dd* y su listado

calcular la duración de la música utilizando el tamaño de las estructuras o tamaño del archivo.

La librería *hachoir-metadata* es utilizada por *Plone4artist*, *django-massmedia* (Librería Open Source del Washigton Post), *amplee* (Implementación del Protocolo de Publicación Atómica, *APP*) y *pyrenamer*. Antes de continuar revisemos de manera breve lo que son los metadatos.

Metadatos

Los metadatos son datos sobre datos. En cómputo forense los metadatos juegan importantes roles, como por ejemplo:

- Pueden proporcionar información que corrobore por sí mismos los datos de un documento.
- Pueden revelar información que alguien intenta ocultar, borrar, u oscurecer.
- Pueden ser utilizados para tener una correspondencia automática de documentos desde diferentes fuentes.

Ya que los metadatos son fundamentalmente datos, pueden ser afectados de los mismas cuestiones relacionadas como cualquier tipo de datos, como por ejemplo la calidad. Sin embargo, debido a que generalmente los metadatos no son visibles, a menos que se utilice una herramienta especial, se requiere de más habilidad para alterarla o manipularla.

Características

Las características más relevantes de *hachoir-metadata* son las siguientes:

- Interfaz Gtk,
- *Plugins* para Nautilus (Gnome) y Konqueror (KDE),
- Soporte para archivos truncados y no válidos,
- Compatible con Unicode (juego de caracteres ISO-8859-XX,

```
Common:
- Duration: 27 sec 320 ms
- Image width: 480 pixels
- Image height: 360 pixels
- Frame rate: 25.0 fps
- Bit rate: 2.8 Mbit/sec
- Producer: Lavf50.6.0
- Comment: Has audio/video index (27.4 KB)
- MIME type: video/x-msvideo
- Endian: Little endian
Video stream:
- Duration: 27 sec 320 ms
- Image width: 480 pixels
- Image height: 360 pixels
- Bits/pixel: 24
- Compression: DivX v3 MPEG-4 Low-Motion (fourcc:"DIV3")
- Frame rate: 25.0 fps
Audio stream:
- Duration: 27 sec 872 ms
- Channel: stereo
- Sample rate: 44.1 kHz
- Compression rate: 11.0x
- Compression: MPEG Layer 3 (fourcc:"\1")
- Bit rate: 128.0 Kbit/sec
```

Figura 5. Información obtenida de un archivo AVI con *hachoir-metadata*

```
root@reydes:[illegible]# hachoir-metadata [illegible]9.JPG
[warn] [/exif/content/ifd[0]/entry[6]/padding] padding contents doesn't look nor
mal (invalid pattern at byte 0)!
Metadata:
- Image width: 294 pixels
- Image height: 448 pixels
- Image orientation: Horizontal (normal)
- Bits/pixel: 24
- Pixel format: YCbCr
- Compression rate: 5.9x
- Image DPI width: 96 DPI
- Image DPI height: 96 DPI
- Creation date: 2009-05-20 16:02:33
- Camera model: DSC-S600
- Camera manufacturer: SONY
- Compression: JPEG (Baseline)
- Producer: Microsoft Windows Photo Gallery 6.0.6000.16386
- Comment: JPEG quality: 98%
- Format version: JFIF 1.01
- MIME type: image/jpeg
- Endian: Big endian
root@reydes:[illegible]#
```

Figura 6. Información obtenida de un archivo JPEG con hachoir-metadata

```
root@reydes:[illegible]# hachoir-metadata --mime *
0901[illegible]9017.mp4: video/quicktime
2976[illegible]23.3gp: video/quicktime
[illegible].wmv: video/x-ms-wmv
46.avi: video/x-msvideo
52968[illegible]06.3gp: video/quicktime
70833[illegible]21.3gp: video/quicktime
[illegible]flv: video/x-flv
[illegible]flv: video/x-flv
[illegible].wmv: video/x-ms-wmv
[illegible]511.jpg: image/jpeg
[illegible]512.jpg: image/jpeg
[illegible]513.jpg: image/jpeg
[warn] Skip parser 'MovFile': False
[illegible].mp4: video/x-flv
[illegible].mpg: video/mpeg
[illegible].wmv: video/x-ms-wmv
[illegible]2.wmv: video/x-ms-wmv
[illegible]2500.flv: video/x-flv
[illegible].png: image/png
[illegible]_1.3gp: video/quicktime
[illegible]_2.3gp: video/quicktime
[illegible](128).3gp: video/quicktime
[illegible](144).3gp: video/quicktime
```

Figura 7. Información obtenida de un archivo JPEG con hachoir-metadata

UTF-8, UTF-16), convierte una cadena en su juego de caracteres terminal,
- Retira valores duplicados (y si una cadena es una subcadena de otra, mantiene la más larga),
- Configura la prioridad para un valor, así es posible filtrar metadatos (opción *–level*),
- Depende solamente de *hachoir-parser* (y no de *libmatroska*, *libmpeg2*, *libvorbis*, etc.).

Formato de archivos soportados

Soporta en total 33 formatos de archivos. A continuación se listan de manera breve:

- Archivos: bzip2, cab, gzip, mar, tar, zip
- Audio: aiff, mpeg_audio ("MP3"), real_audio (RA), sun_next_snd, MIDI, AIFC
- Contenedores: matroska, ogg, real_media, riff
- Imagen: bmp, gif, ico, jpeg, pcx, png, psd, targa, tiff, wmf, xcf
- Varios: ole2, pcf, torrrent, ttf
- Programa: exe
- Vídeo: asf (video WMV), flv, mov, AVI.

Modos

Hachoir-metadata tiene tres modos:

- *Modo clásico*: extrae metadatos, se puede utilizar *--level=LEVEL* para limitar la cantidad de información que se muestra,
- `--type`: muestra en una línea el formato de archivo y la información más importante,
- `--mime`: muestra solamente el tipo de archivo MIME.

El comando *hachoir-metadata --mime* funciona como *file --mime*, y *hachoir-metadata --type* como *file*. Pero en la actualidad el comando *file* soporta más formatos de archivos que *hachoir-metadata*.

```
root@reydes:/media/hda3# hachoir-subfile hdb.dd --parser=jpeg | more
[+] Start search on 6448619520 bytes (6.0 GB)

[+] File at 253440 size=56987 (55.7 KB): JPEG picture
[+] File at 353804 size=1750 (1750 bytes): JPEG picture
[+] File at 355596: JPEG picture
[+] File at 400896 size=2404 (2404 bytes): JPEG picture
[+] File at 809420 size=3097 (3097 bytes): JPEG picture
[+] File at 813580 size=3080 (3080 bytes): JPEG picture
[+] File at 816972 size=236073 (230.5 KB): JPEG picture
[+] File at 2737676 size=61874 (60.4 KB): JPEG picture
[+] File at 3878400 size=26283 (25.7 KB): JPEG picture
[+] File at 6733312 size=15988 (15.6 KB): JPEG picture
[+] File at 8060416 size=19496 (19.0 KB): JPEG picture
[+] File at 9559552 size=26595 (26.0 KB): JPEG picture
[+] File at 9979404 size=29624 (28.9 KB): JPEG picture
[+] File at 11386368 size=215450 (210.4 KB): JPEG picture
[+] File at 11648512 size=157198 (153.5 KB): JPEG picture
[+] File at 13774336 size=64835 (63.3 KB): JPEG picture
[+] File at 14896642 size=25537 (24.9 KB): JPEG picture
[+] File at 18873856 size=24605 (24.0 KB): JPEG picture
[+] File at 19549696 size=42228 (41.2 KB): JPEG picture
[+] File at 20983296 size=5169 (5169 bytes): JPEG picture
[+] File at 22533132 size=231227 (225.8 KB): JPEG picture
```

Figura 9. Búsqueda de archivos JPEG con *hachoir-subfile*

```
root@reydes:[illegible]# hachoir-metadata --type *
0905[illegible].mp4: Apple QuickTime movie
2978[illegible].3gp: Apple QuickTime movie
[illegible].wmv: Window Media Video (wmv)
46.avi: Microsoft AVI video: 320x240 pixels, 30.0 fps, 3 years 290 days 9 hours
520[illegible]206.3gp: Apple QuickTime movie
70[illegible]721.3gp: Apple QuickTime movie
[illegible].flv: Macromedia Flash video version 1
[illegible].flv: Macromedia Flash video version 1
[illegible]: Window Media Video (wmv)
[illegible]1511.jpg: JPEG picture
[illegible]1512.jpg: JPEG picture
[illegible]11513.jpg: JPEG picture
[warn] Skip parser 'MovFile': False
[illegible]mp4: Macromedia Flash video version 1
[illegible].mpg: MPEG-1 video
[illegible].wmv: Window Media Video (wmv)
[illegible]_2.wmv: Window Media Video (wmv)
[illegible].flv: Macromedia Flash video version 1
[illegible].png: PNG picture: 96x96x32 (alpha layer)
[illegible]1.3gp: Apple QuickTime movie
[illegible]_2.3gp: Apple QuickTime movie
[illegible](128).3gp: Apple QuickTime movie
[illegible](144).3gp: Apple QuickTime movie
```

Figura 8. Información expuesta por *hachoir-metadata --type* en los archivos de un directorio

Ejemplos prácticos

Para iniciar los ejemplos prácticos con los programas del presente artículo, se tiene el siguiente escenario. Una imagen bit a bit de nombre *hdb.dd,* con hash MD5; 7a31655a4d6381744d6efb2f9205bb9a. Con una estructura de particiones y sistemas de archivos los cuales se muestran en la Figura 3. Cuando sea necesario realizar el montaje de esta imagen bit a bit, éste se realizará respetando las buenas prácticas forenses en lo que respecta al comando *mount* en GNU/Linux.

Se ha procedido a montar las dos particiones contenidas en la imagen bit a bit *hdb.dd* con los siguientes comandos:

```
# mount -o ro,loop,offset=32256 -t auto hdb.dd s_hdb1/
# mount -o ro,loop,offset=3298369536 -t auto hdb.dd
s_hdb5/
```

En la Figura 4 se muestran los comandos utilizados para realizar el montaje y también el listado de sus carpetas y archivos de sus directorios raíz. Se procede a obtener información mediante *hachoir-metadata* de unos de los archivos AVI (formato de archivo RIFF) encontrado en el sistema de archivos, tal y como lo muestra la Figura 5, con el siguiente comando: `# hachoir-metadata infraganti.avi.`

A continuación se analiza la información que se muestra en la Figura 5, así se puede comprender mejor la importancia de los metadatos en cómputo forense.

Información ordinaria:

- La duración del archivo es de 27 segundos y 320 milisegundos,
- El ancho de la imagen es de 480 pixeles,
- El alto de la imagen es de 360 pixeles,
- El *Frame rate* o Frecuencia de cuadros es de 25.0 fps (cuadros por segundo),
- El *Bit rate* o Frecuencia de Bits es de: 2.8 Mbit/seg,
- El Productor es Lavf50.6.0,

```
root@reydes:/media/hda3# hachoir-subfile hdb.dd --category=image | more
[+] Start search on 6448619520 bytes (6.0 GB)

[+] File at 105984 size=3894 (3894 bytes): Microsoft Bitmap version 3
[+] File at 109887 size=2358 (2358 bytes): Microsoft Bitmap version 3
[+] File at 155136 size=12765 (12.5 KB): PNG picture: 96x96x32 (alpha layer)
[+] File at 216576 size=152744 (149.2 KB): PNG picture: 96x96x32 (alpha layer)
[+] File at 253440 size=56987 (55.7 KB): JPEG picture
[+] File at 253470: TIFF picture
[+] File at 290304 size=79016 (77.2 KB): PNG picture: 86x128x32 (alpha layer)
[+] File at 353804 size=1750 (1750 bytes): JPEG picture
[+] File at 355596: JPEG picture
[+] File at 359936 size=9384 (9384 bytes): PNG picture: 96x96x24
[+] File at 400896 size=2404 (2404 bytes): JPEG picture
[+] File at 441856 size=363753 (355.2 KB): PNG picture: 128x95x32 (alpha layer)
[+] File at 809420 size=3097 (3097 bytes): JPEG picture
[+] File at 813580 size=3080 (3080 bytes): JPEG picture
[+] File at 816972 size=236073 (230.5 KB): JPEG picture
[+] File at 818690 size=24056 (23.5 KB): PNG picture: 96x96x32 (alpha layer)
[+] File at 835072 size=7674 (7674 bytes): PNG picture: 128x93x32 (alpha layer)
[+] File at 1019392 size=16867 (16.5 KB): PNG picture: 128x102x32 (alpha layer)
[+] File at 1068544 size=285054 (278.4 KB): PNG picture: 96x96x32 (alpha layer)
[+] File at 1097216 size=256382 (250.4 KB): PNG picture: 95x128x32 (alpha layer)
[+] File at 1269248 size=84350 (82.4 KB): PNG picture: 96x96x32 (alpha layer)
```

Figura 10. Búsqueda de los tipos de archivo de imágenes con hachoir-subfile

```
root@reydes:/media/hda3# hachoir-subfile hdb.dd /tmp/archivos
[+] Start search on 6448619520 bytes (6.0 GB)

[+] File at 32256: NTFS file system
[+] File at 40451 size=290784546142618369 (264467 TB): ChmFile (don't copy file,
 too big)
[+] File at 105984 size=3894 (3894 bytes): Microsoft Bitmap version 3 => /tmp/ar
chivos/file-0001.bmp
[+] File at 109887 size=2358 (2358 bytes): Microsoft Bitmap version 3 => /tmp/ar
chivos/file-0002.bmp
[+] File at 155136 size=12765 (12.5 KB): PNG picture: 96x96x32 (alpha layer) =>
/tmp/archivos/file-0003.png
[+] File at 192003 size=290784546142618369 (264467 TB): ChmFile (don't copy file
, too big)
[+] File at 216576 size=152744 (149.2 KB): PNG picture: 96x96x32 (alpha layer) =
> /tmp/archivos/file-0004.png
[+] File at 220675 size=290784546142618369 (264467 TB): ChmFile (don't copy file
, too big)
[+] File at 253440 size=56987 (55.7 KB): JPEG picture => /tmp/archivos/file-0005
.jpg
[+] File at 253470: TIFF picture
[+] File at 290304 size=79016 (77.2 KB): PNG picture: 86x128x32 (alpha layer) =>
 /tmp/archivos/file-0006.png
[err!] [/] FAT chain: list index out of range
```

Figura 11. Búsqueda de todos los archivos y extracción en la carpeta */tmp/archivos*

- Se incluye el siguiente comentario: tiene un índice de audio/video (27.4 KB),
- El Tipo MIME (Extensiones de Correo de Internet Multipropósito) es video/x-msvideo,
- Endian: Little endian. Implica que los bytes menos significativos son almacenados en las direcciones de memoria más baja.

Flujo de Vídeo:

- La duración del vídeo es 27 segundos y 320 milisegundos,
- El ancho de la imagen es de 480 pixeles,
- El alto de la imagen es de 360 pixeles,
- Los bits por pixel es de 24,
- La información de compresión es DivX v3 MPEG-4 Low-Motion (fourcc:"DIV3"),
- La frecuencia de marcos es de: 25.0 cps.

Flujo de Audio:

- La duración del audio es 27 segundos y 872 milisegundos,
- Canal: estéreo,
- La frecuencia de la muestra es de 44.1 kHz,
- La frecuencia de compresión es de 11.0x,
- La información de compresión es MPEG Layer 3 (fourcc:"\1"),
- La frecuencia de bits es 128.0 Kbit/sec.

A continuación se procede a utilizar *hachoir-metadata* en uno de los archivos de formato JPEG. La información obtenida se puede visualizar en la Figura 6. A continuación se analiza la información obtenida con el comando:

```
# hachoir-metadata figura9.JPG
```

```
0) file=[illegible].avi: Microsoft AVI video: 480x360 pixels, 25.0 fp
   0) signature= "RIFF": AVI header (RIFF) (4 bytes)
   4) filesize= 9.1 MB: File size (4 bytes)
   8) type= "AVI ": Content type ("AVI ", "WAVE", ...) (4 bytes)
 - 12) headers: Headers (8830 bytes)
     0) tag= "LIST": Tag (4 bytes)
     4) size= 8822 bytes: Size (4 bytes)
     8) subtag= "hdrl": Sub-tag (4 bytes)
   + 12) avi_hdr: AVI header (64 bytes)
   - 76) stream[0]: Stream header list (4248 bytes)
       0) tag= "LIST": Tag (4 bytes)
       4) size= 4240 bytes: Size (4 bytes)
       8) subtag= "strl": Sub-tag (4 bytes)
     - 12) stream_hdr: Stream header (64 bytes)
         0) tag= "strh": Tag (4 bytes)
         4) size= 56 bytes: Size (4 bytes)
         8) stream_type= "vids": Stream type four character code (4 bytes)
         12) fourcc= DivX v3 MPEG-4 Low-Motion: Stream four character code (4
         16) flags= 0: Stream flags (4 bytes)
         20) priority= 0: Stream priority (2 bytes)
         22) language= (empty): Stream language (2 bytes)
         24) init_frames= 0: InitialFrames (4 bytes)
         28) scale= 1: Time scale (4 bytes)
 0 root                                          log: 0/0/0 | F1: help
```

Figura 13. Explorando el archivo *infraganti.avi* con *Hachoir-urwiv*

```
root@reydes:/media/hda3# hachoir-subfile --offset=3298369536 hdb.dd
[+] Start search on 3150249984 bytes (2.9 GB)

[+] File at 3298369536: FAT32 filesystem
[+] File at 3298372608: FAT32 filesystem
[+] File at 3298740528 size=11835905 (11.3 MB): MS-DOS executable
[+] File at 3300313392 size=11835911 (11.3 MB): MS-DOS executable
[+] File at 3301361968 size=11835915 (11.3 MB): MS-DOS executable
[+] File at 3301814064 size=11835905 (11.3 MB): MS-DOS executable
[+] File at 3303386928 size=11835911 (11.3 MB): MS-DOS executable
[+] File at 3304435504 size=11835915 (11.3 MB): MS-DOS executable
[+] File at 3304594432 size=18432 (18.0 KB): Microsoft Windows Portable Executab
le: Intel 80386, Windows CUI
[+] File at 3304639488 size=30481 (29.8 KB): JPEG picture
[+] File at 3304672256 size=15675 (15.3 KB): JPEG picture
[+] File at 3304688640 size=80384 (78.5 KB): Microsoft Windows Portable Executab
le: Intel 80386, Windows CUI
[+] File at 3304770560 size=65536 (64.0 KB): Microsoft Windows Portable Executab
le: Intel 80386, Windows CUI
[+] File at 3304836096 size=146432 (143.0 KB): Microsoft Windows Portable Execut
able: Intel 80386, Windows CUI
[+] File at 3304983552 size=24064 (23.5 KB): Microsoft Windows Portable Executab
le: Intel 80386, Windows CUI
[+] File at 3305008128 size=21504 (21.0 KB): Microsoft Windows Portable Executab
```

Figura 12. Búsqueda de archivos en un desplazamiento definido en bytes

Metadatos:

- El ancho de la imagen es de 294 pixeles,
- El alto de la imagen es de 448 pixeles,
- La orientación de la imagen es la normal: *Horizontal,*
- Los bits por pixel es de 24,
- El formato del pixel es YCbCr,
- La frecuencia de compresión es de 5.9x,
- El ancho en Puntos por Pulgada (DPI) de la imagen es de 96 DPI,
- El alto en Puntos por Pulgada (DPI) de la imagen es de 96 DPI,
- La fecha de creación es 2009-05-20 16:02:33,
- El modelo de la cámara es DSC-S600,
- El fabricante de la cámara es SONY,
- La comprensión es JPEG (Baseline),
- El productor es Microsoft Windows Photo Gallery 6.0.6000.16386,
- Comentario: JPEG quality: 98%,
- Versión del formato JFIF 1.01,
- El tipo MIME (Extensiones de Correo de Internet Multipropósito) es image/jpeg,
- Endian: Big endian. Implica que los bytes más significativos son almacenados en las direcciones de memoria más baja.

Como se puede inferir hasta el momento, los metadatos exponen información de mucha utilidad para el investigador forense, dado que esta información como ya se explicó, puede ayudar a corroborar información del archivo por sí mismo, y poder ser utilizado para ser relacionado con otro tipo de información.

La opción *--mime* muestra solamente la información del tipo MIME, trabaja como el comando *file --mime* en GNU/Linux. La Figura 7 muestra el resultado de aplicar este comando a todos los archivos en un directorio. La opción *--type* muestra una corta descripción del tipo de archivo, como el comando *file* en GNU/Linux. La Figura 8 muestra el resultado del comando antes mencionado aplicado a los mismos archivos del directorio utilizado para el comando anterior.

```
      8) version= 42: TIFF version number (2 bytes)
      10) img_dir_ofs= 8: Next image directory offset (4 bytes)
    - 14) ifd[0]: IFD (6682 bytes)
        0) count= 12: Number of entries (2 bytes)
      + 2) entry[0]: Entry: Image title (12 bytes)
      + 14) entry[1]: Entry: Camera (Image input equipment) manufacturer (12
      + 26) entry[2]: Entry: Camera (Input input equipment) model (12 bytes)
      + 38) entry[3]: Entry: Orientation of image (12 bytes)
      + 50) entry[4]: Entry: Software (12 bytes)
      + 62) entry[5]: Entry: File change date and time (12 bytes)
      + 74) entry[6]: Entry: Y and C positioning (12 bytes)
      + 86) entry[7]: Entry: Exif IFD Pointer (12 bytes)
      + 98) entry[8]: Entry: 0x9c9e (12 bytes)
      + 110) entry[9]: Entry: 0xc4a5 (12 bytes)
      + 122) entry[10]: Entry: 0xea1c (12 bytes)
      + 134) entry[11]: Entry: 0xea1d (12 bytes)
        146) next= 0: Next IFD offset (4 bytes)
        150) value_entry[10]= "\x1c\xea\0\0\0\b\0\0\0\0\0\0\0\0(...)": Value
        2210) value_entry[0]= (empty): Value of "Image title" (32 bytes)
        2242) value_entry[1]= "SONY": Value of "Camera (Image input equipmen
        2247) padding[0]= "\0" (1 byte)
        2248) value_entry[2]= "DSC-S600": Value of "Camera (Input input equi
        2257) padding[1]= "\0" (1 byte)
 0 root                                          log: 0/1/0 | F1: help
```

Figura 14. Explorando el archivo *Figura9.JPG* con *Hachoir-urwiv*

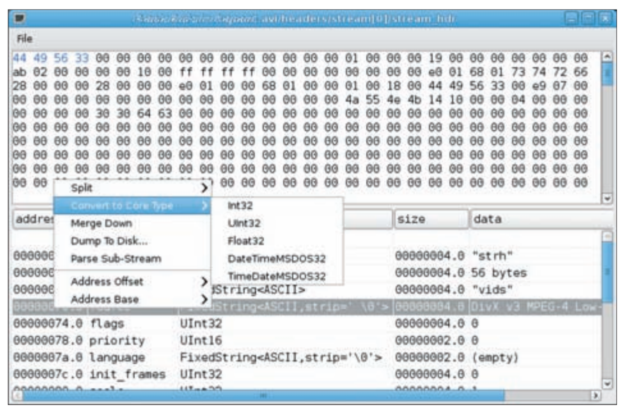


Figura 15. Explorando el archivo *infraganti.avi* con *Hachoir-wx*

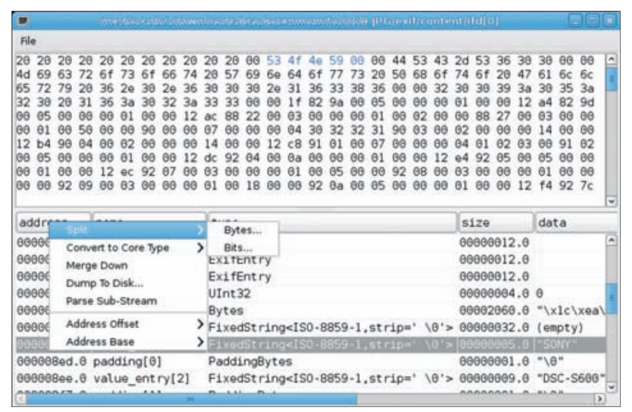


Figura 16. Explorando el archivo *Figura9.JPG* con *Hachoir-wx*

Finalmente *Hachoir-metadata*, permite definir la cantidad de información a mostrar mediante la opción *–level=[1-9]*, siendo 9 lo máximo, visualizar la salida en bruto con la opcion *–raw,* definir la calidad de la información mostrada con la opción *--quality=[0.0-1.0]*, siendo 0.5 lo que se utiliza por defecto; definir la longitud máxima de caracteres mediante el parámetro *--maxlen=LONGITUD*, 0 significa sin límite, y 300 se usa por defecto. Finalmente tres opciones también relevantes: *--verbose* que muestra información abundante sobre el proceso; *--log=LOG* que permite escribir un archivo de registro "LOG" y finalmente un modo de depuración *--debug*.

hachoir-parser

hachoir-parser es un paquete de los intérpretes de los formatos de archivo más comunes, escrito para el *framework* de *Hachoir*. No todos los intérpretes están completos, algunos son muy buenos y otros pobres (por ejemplo sólo interpretan el primer nivel de los tres existentes).

Un intérprete perfecto no tiene un campo "raw" (en bruto): con un intérprete perfecto es posible conocer el significado de cada bit. Algunos de los intérpretes buenos (pero no perfectos) son:

- Matroska video,
- Microsoft RIFF (AVI video, WAV audio, archivo CDA),
- Imagen PNG,
- Archivo TAR y ZIP.

El intérprete *GnomeKeyring* requiere el módulo Ptyhon Cryptography.

Gnome Keyring es un lugar donde se almacenan en un archivo cifrado las contraseñas (y pronto las claves de cifrado) de un usuario. El usuario ingresa una contraseña global cuando accede por primera vez. Finalmente detallar que el módulo *Python Cryptography* es una colección de algoritmos y protocolos de cifrado, para ser utilizados por Python.

```
root@reydes:~/tools/forensics/hachoir/hachoir-tools# less README.hachoir-strip
root@reydes:~/tools/forensics/hachoir/hachoir-tools# ./hachoir-strip [illegible]
[illegible]i_copia.avi
[+] Process file [illegible]i_copia.avi
Remove field /headers/stream[0]/junk[0]
Remove field /headers/stream[1]/junk[0]
Remove field /headers/junk[0]
Remove field /info
Remove field /junk[0]
Remove field /index
Remove 36.7 KB (0.4%)
Save new file into [illegible]i_copia.avi.ne
w
root@reydes:~/tools/forensics/hachoir/hachoir-tools# ./hachoir-strip [illegible]
[illegible]9_copia.JPG
[+] Process file [illegible]9_copia.JPG
Remove field /exif
Remove 6700 bytes (8.5%)
Save new file into [illegible]9_copia.JPG.new
root@reydes:~/tools/forensics/hachoir/hachoir-tools#
```

Figura 17. Ejecución de *hachoir-strip* en los archivos *infraganti_copia.avi* y *Figura9_copia.JPG*

Lista de intérpretes

Los siguiente son los 70 intérpretes:

- Archivo: 7zip, ace, bzip2, cab, gzip, mar, rar, rpm, tar, unix_archive, zip
- Audio: aiff, fasstracker2, itunesdb, midi, mod, mpeg_audio,ptm, real_audio, s3m, sun_next_snd
- Contenedor: asn1, matroska, ogg, ogg_stream, real_media_riff_swf
- Sistema de Archivo: ext2, fat12, fat16, fat32, iso 9660, linux_swap, msdos_harddrive, ntfs, reiserfs
- Juego: lucasarts_font, spiderman_video, zsness
- Imagen: bmp, gif, ico, jpeg, pcx, png, psd, targa, tiff, wmf, xcf
- Varios: 3do, 3ds, chm, lnk, ole2, pcf, pdf, tcpdump, torrent, ttf
- Programa: elf, exe, java_class, python
- Video: asf, flv, mov, mpeg_ts_ mpeg_video

Extensiones de archivo soportados

En total son 135 extensiones de archivos, que se detallan a continuación: 3do, 3ds, 7z, a, ace, aif, aifc, aiff, ani, apm, asf, au, avi, bin, bmp, bz2, cab, cda, chm, class, cur, deb, der, dll, doc, dot, emf, exe, flv, gif, gz, ico, jar, jpeg, jpg, laf, lnk, m4a, m4b, m4p, m4v, mar, mid, midi, mka, mkv, mod, mov, mp1, mp2, mp3, mp4, mpa, mpe, mpeg, mpg, msi, nst, oct, ocx, odb, odc, odf, odg, odi, odm, odp, ods, odt, ogg, ogm, otg, otp, ots, ott, pcf, pcx, pdf, png, pot, pps, ppt, ppz, psd, ptm, pyc, pyo, qt, ra, rar, rm, rpm, s3m, sd0, snd, so, stc, std, sti, stw, swf, sxc, sxd, sxg, sxi, sxm, sxw, tar, tga, tif, tiff, torrent, ts, ttf, vob, wav, wma, wmf, wmv, wow, xcf, xla, xls, xm, zip, zs1, zs2, zs3, zs4, zs5, zs6, zs7, zs8, zs9, zst.

Finalmente los tipos MIME soportados, que son 116, se han obviado por cuestiones de espacio. Sugiero consultar la página del proyecto para obtener el listado completo.

```
root@reydes:~/tools/forensics/hachoir/hachoir-tools# hachoir-metadata [illegible]
[illegible]i_copia.avi.new
Common:
- Duration: 27 sec 320 ms
- Image width: 480 pixels
- Image height: 360 pixels
- Frame rate: 25.0 fps
- Bit rate: 2.8 Mbit/sec
- MIME type: video/x-msvideo
- Endianness: Little endian
Video stream:
- Duration: 27 sec 320 ms
- Image width: 480 pixels
- Image height: 360 pixels
- Bits/pixel: 24
- Compression: DivX v3 MPEG-4 Low-Motion (fourcc:"DIV3")
- Frame rate: 25.0 fps
Audio stream:
- Duration: 27 sec 872 ms
- Channel: stereo
- Sample rate: 44.1 kHz
- Compression rate: 11.0x
- Compression: MPEG Layer 3 (fourcc:"\1")
- Bit rate: 128.0 Kbit/sec
```

Figura 18. Ejecución de *hachoir-metadata* en el archivo *infraganti_copia.avi.new*

hachoir-subfile

hachoir-subfile es una herramienta basada en *hachoir-parser* para encontrar sub archivos en un flujo binario.

¿Cómo funciona?

Primero se presentará de manera breve el concepto de número mágico (Magic Number): Número Mágico es una forma de identificar el formato de un archivo es almacenar información relacionada al formato del archivo dentro del archivo mismo, tal información se escribe en una (o más) cadenas binarias que se colocan en lugares fijos etiquetados o en texto plano. Ya que el lugar más fácil de colocar esto es al inicio del archivo, usualmente tal área se denomina como la *cabecera del archivo* cuando es mayor de algunos bytes, o un *número mágico* cuando tiene pocos bytes de longitud.

Originalmente, el término fue utilizado para especificar un conjunto de identificadores de 2 bytes al principio de un archivo, pero cualquier secuencia binaria decodificada puede ser relacionada como tal número, así mismo cualquier característica de un formato de archivo el cual lo distingue de manera única puede ser utilizada para la identificación.

Ubicando el inicio

Para ubicar el inicio, *hachoir-subfile* utiliza el "número mágico". Ejemplos:

- "MZ" para ejecutables MS-DOS y (y Windows),
- "\xFF\xD8\xFF" para JPEG,
- "FAT16 " para sistema de archivo FAT16.

Cuando se encuentra el número mágico, se abre un intérprete de *hachoir-parser*. Luego se utiliza el método *validate()* para asegurar que el archivo está en el formato de archivo correcto. Algunos valores de la cabecera que son evaluados, son:

- Archivo TAR: comprueba el número mágico, comprueba la entrada del primer archivo (identificador del usuario/grupo, tamaño del archivo),
- Animación SWF: comprueba el número mágico, comprueba la versión, comprueba el valor del relleno del rectángulo.
- etc.

Ubica la longitud:

Para encontrar (adivinar) la longitud del archivo, cada intérprete requiere un método llamado "*createContentSize()*". Ejemplos:

- Contenedor RIFF: lee el valor de campo "/filesize"
- Imagen JPEG: busca la cadena "\xFF\xD9" (final del trozo de la imagen)
- etc.

Ejemplos prácticos

Siguiendo con el escenario ya descrito para la aplicaciones prácticas con *Hachoir*. Es el turno de exponer algunos ejemplos con *hachoir-subfile*.

La búsqueda de imágenes JPEG se realiza con el siguiente comando:

```
# hachoir-subfile hdb.dd --parser=jpeg
```

En los resultados expuestos por la Figura 9, se puede visualizar un número que indica el desplazamiento donde se ubica la cabecera del archivo, el tamaño del archivo en bytes y Kb, además del tipo de archivo. Como se puede apreciar también, no siempre se puede detectar un archivo JPEG con precisión, es por este motivo que en ciertas situaciones sólo se indica que se trata de una imagen JPEG, mas no se exponen datos como el tamaño, esto a razón de la imposibilidad de encontrar el "pie" del archivo.

La búsqueda de todas las imágenes que son factibles de reconocer como tal, se realiza con el siguiente comando:

```
# hachoir-subfile hdb.dd --category=image
```

Como se puede apreciar en los resultados obtenidos, véase la Figura 10, de esta manera es factible ubicar todos los tipos de archivos de imagen que *Hachoir-subfile* es capaz de reconocer como tales. Se incluye en los resultados la información expuesta como el tipo de archivo, y en algunos casos el tamaño y resolución de la imagen.

Es posible también realizar la búsqueda de todos los sub archivos y almacenar una copia de éstos en un directorio (*/tmp/archivos*), tal y como se muestra en la Figura 11.

```
# hachoir-subfile hdb.dd /tmp/archivos
```

Para iniciar la búsqueda en un desplazamiento en bytes definido se puede utilizar la opción *--offset* de la siguiente manera:

```
# hachoir-subfile --offset=3298369536 hdb.dd
```

Como se puede visualizar en la Figura 12, en las primera líneas que corresponden a los resultados se expone el reconocimiento de un Sistema de Archivos de tipo FAT32. Esto a razón de que en la opción *offset* se ha definido el número que corresponde al desplazamiento donde inicia una partición conteniendo este tipo de sistema de archivos. Por lo tanto es factible analizar los archivos que residen en una partición determinada.

Para los lectores que hayan utilizado herramientas de recuperación de archivos a bajo nivel, como por ejemplo *foremost* o *scalpel,* resulta más fácil comprender el funcionamiento de *hachoir-subfile*. Creo conveniente mencionar que en un anterior número de Linux+, escribí un artículo sobre *Foremost y Scalpel*, cuya lectura recomiendo.

```
root@reydes:~/tools/forensics/hachoir/hachoir-tools# hachoir-metadata
[illegible]i9_copia.JPG.new
Metadata:
- Image width: 294 pixels
- Image height: 448 pixels
- Bits/pixel: 24
- Pixel format: YCbCr
- Compression rate: 5.9x
- Image DPI width: 96 DPI
- Image DPI height: 96 DPI
- Compression: JPEG (Baseline)
- Comment: JPEG quality: 98%
- Format version: JFIF 1.01
- MIME type: image/jpeg
- Endianness: Big endian
root@reydes:~/tools/forensics/hachoir/hachoir-tools#
```

Figura 19. Ejecución de *hachoir-metadata* en los archivos *Figura9_copia.JPG.new*



hachoir-urwid

Hachoir-urwid es un explorador de archivos binarios basado en la librería *Hachoir* para interpretar los archivos. Con la utilización de esta herramienta se puede conocer exactamente el significado de cada bit/byte de los archivos. Con las teclas de dirección, se puede navegar en el árbol de campos. Por ejemplo la tecla "h" inhabilitará la "visualización humana", y cambiará hacía la visualización en bruto. Esto es útil algunas veces cuando se desea comparar datos en hexadecimal y la representación de Hachoir.

Opciones de inicio

Es factible iniciar *Hachoir-urwid* con las siguientes opciones de inicio:

- `--preload=10`: carga diez campos cuando se carga un nuevo conjunto de campos
- `--path="header/bpp"`: abre la ruta especificada y se enfoca en el campo
- `--parser=PARSERID`: fuerza el intérprete (y evita la validación de intérprete)

Teclas útiles

Mover:

- up/down: mover arriba/abajo
- home: va al padre
- end: va al último campo de un conjunto de campos
- left/right: desplazamiento horizontal

Configuración de pantalla:

- h: la opción más importante, cambia entre pantalla humana (por defecto, es decir comprensible para un humano) y valor en bruto
- v / d / s: muestra u oculta el valor de campo / descripción / tamaño
- a: cambia entre dirección relativa (por defecto) y absoluta
- b: cambia entre dirección en decimal (por defecto) y hexadecimal

Interacción:

- enter: sobre un conjunto de campos, expande o colapsa el hijo
- space: interpreta el archivo / flujo contenido en el campo actual

Aplicación:

- q: salir
- < / >: tabular entre previo / siguiente
- + / -: mover verticalmente separador
- esc o CTRL+W: cierra el tabulador actual
- F1: muestra la ayuda

Ejemplos prácticos

Para seguir con el flujo consecuente de los ejemplos antes descritos, se utilizan los mismos archivos *infraganti.avi* y *Figura9.JPG*, con *hachoir-urwid*.

```
# hachoir-urwid infraganti.avi
```

La Figura 13, muestra cómo se explora el archivo de nombre *infraganti.avi*. Por ejemplo en la imagen se puede apreciar como se estructuran los campos en un archivo AVI. Es obvio, que para tener una comprensión cabal de lo que *hachoir-urwiv* presenta, es necesario estar familiarizado con la estructura interna del archivo que está siendo analizado. En este caso se observan datos importantes: se trata de un video AVI Microsoft, con medidas de ancho y alto de 480x360 pixeles, de 25 cuadros por segundo. Además un campo con su firma que lo identifica como RIFF, un campo correspondiente al tamaño del archivo, que es de 9.1Mb. También es factible observar la información de la compresión *DivX v3 MPEG-4 Low-Motion*, entre muchos campos y grupos de campos que el analista forense debe de comprender para poder realizar un análisis adecuado:

```
# hachoir-urwid Figura9.JPG
```

En la Figura 14 se puede apreciar parte de los campos del archivo *Figura9.JPG*, se ha procedido a ubicar a *Hachoir-urwid* en aquellos campos donde se revela información como el fabricante de la cámara, en este caso SONY, información del modelo de la cámara, DSC-S600. Se reitera lo dicho anteriormente, para comprender cabalmente este tipo de análisis es necesario comprender cómo se estructuran los campos en un tipo de archivo JPEG.

En la parte de referencias del presente artículo se detallan dos enlaces con información importante sobre la estructura tanto de los archivos AVI como JPEG.

hachoir-wx

Hachoir-wx es un programa basado en *wxWidgets* que intenta proporcionar una interfaz (más) amigable a las facilidades proporcionadas por el núcleo del interprete binario. Algunas de sus características son:

- GUI Interfaz Gráfica de Usuario basado en *wxWidgets,*
- La versión actual es experimental y no muy estable,
- Existen ocasiones (con suerte) que se hacen pequeñas revisiones de código mientras el código es progresivamente refactorizado. Es un proceso de aprendizaje, o algo similar,
- La organización del código es la principal prioridad.

Ejemplos prácticos

`hachoir-wx infraganti.avi y hachoir-wx Figura9.JPG`

En la Figura 15 se pueden visualizar los mismo campos que se han detallado en los ejemplos anteriores, los cuales corresponden al archivo *infraganti.avi*. Como se puede apreciar en la imagen, este entorno visual tiene interesantes características, como separar en bytes y bits, fusionar, hacer un volcado en disco, interpretar un subflujo, y claro está la opción seleccionada en la imagen, que implica conversión del tipo a *Int32*, *Uint32*, *Float32*, *DateTimeMSDOS32*, *TimeDateMSDOS32*.

En la Figura 16 también se ha procedido a seleccionar la misma ubicación del archivo *Figura9.JPG* analizado anteriormente con *hachoir-urwid*. En este caso se puede apreciar que se ha seleccionado la opción *Split,* dividir o separar, la cual permite hacerlo en Bytes o Bits.

hachoir-strip

Durante el transcurso del presente artículo se ha presentado *Hachoir* como un mecanismo para extraer y analizar información de archivos binarios. Pero existe un programa experimental denominado *Hachoir-strip,* basado en la librería *Hachoir,* el cual retira información

"inútil" de un archivo. Como se comprenderá esta información denominada como "inútil", puede ser de mucha utilidad para el investigador forense, y la utilización de este programa puede complicar su trabajo.

Opciones

Las opciones de *hachoir-strip* son muy simples:

- La opción por defecto retira todos los campos "inútiles",
- `--strip=useless`: retira todos los campos inútiles (ejemplo, de relleno),
- `--strip=metadata`: retira metadatos como etiquetas ID3 y metadatos EXIF y IPTC,
- `--strip=index`: retira el indice de un vídeo.

Las opciones anteriormente descritas pueden combinarse separadas por comas.

Ejemplos prácticos

Se ha procedido a realizar una copia de los archivos que se han utilizado durante el transcurso del presente artículo, los nuevos nombres de los archivos son *infraganti_copia.avi* y *Figura9_copia.AVI.* Pero se debe tener en consideración que luego de la ejecución de *hachoir-strip*, se creará un nuevo archivo con extensión *.new,* el cual es el archivo procesado pero sin la información "inútil".

Los comandos a utilizar para retirar la información "inútil" de ambos archivos son los siguientes:

```
# ./hachoir-strip infraganti_copia.avi
# ./hachoir-strip Figura9_copia.JPG
```

En la Figura 17 se pueden apreciar los mensajes expuestos tras la ejecución de *hachoir-strip* para cada uno de los archivos, donde se detallan los campos "inútiles" que han sido retirados.

También es factible crear un hash MD5 a los archivos obtenidos de extensión *.new,* y comparar estos *hashs*, con los *hashs* obtenidos de los archivos originales. Con una simple acción es factible detectar que los nuevos archivos han sufrido modificaciones respecto a su original:

```
# md5sum infraganti_copia.avi
57cfa07fe91edea330b9ff4b92bcc453
# md5sum infraganti.avi.new
f7a8193c336eed77c5256e0b118560f5
# md5sum Figura9.JPG
d721f390148f9d253ec9f4574aede02b
# md5sum Figura9.JPG.new
9c1caaf1c71f0a1cd0ca083e497ab5fd
```

En la Figura 18 se pueden observar los resultados obtenidos luego de la ejecución de *hachoir-metadata* sobre el archivo *infraganti_copia.avi.new*. En este caso no es muy notorio percatarse de la eliminación del campo denominado *Productor (Producer)*.

Pero por contraparte en la Figura 19, se pueden visualizar los resultados obtenidos luego de la ejecución de *hachoir-metadata* al archivo *Figura9_copia.JPG.new,* donde sí es bastante notoria la eliminación de información "inútil", como por ejemplo, fecha de creación, modelo de la cámara, fabricante de la cámara y productor.

Existen otros programas que no se han detallado en el presente artículo y que invito a configurar y utilizar. Por ejemplo *hachoir-editor* para editar archivos binarios, *hachoir-regex* que permite la manipulación de expresiones regulares; entre otros programas. Solamente me resta invitar a "jugar" con estas herramientas, pues es la mejor manera de aprender sobre ellas.

Conclusiones

El adjetivo o la frase de que Hachoir es una navaja suiza para los archivos binarios, me parece muy acertada. Como se puede apreciar en el presente artículo, dispone de variados programas que permiten realizar diversas tareas que competen al campo del análisis forense.

Para obtener todo el potencial de *hachoir* se deben tener claros conceptos forenses, como por ejemplo la estructura de los sistemas de archivos, metadatos de un archivo, *endian*, conceptos de cabeceras y pies, entre otros.

Las herramientas, como *hachoir* en este caso, son solamente un mecanismo para facilitar y optimizar el trabajo del analista forense, pues es éste el encargado de analizar e interpretar de manera adecuada la evidencia forense obtenida por las herramientas.



Sobre el Autor

Alonso Eduardo Caballero Quezada es Brainbench Certified Computer Forensics (U.S.) y GIAC SSP-CNSA. Actualmente labora como consultor en Cómputo Forense y Hacking Ético. Perteneció por muchos años al grupo RareGaZz. Actualmente es integrante del Grupo Peruano de Seguridad PeruSEC. Se presenta de manera frecuente en cursos y ponencias, las cuales se enfocan en Cómputo Forense, Hacking Ético, Análisis de Vulnerabilidades, Pruebas de Penetración, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: *http://www.ReYDeS.com.*



En la red

- Hachoir – *http://bitbucket.org/haypo/hachoir/*
- Hachoir – Forensics Wiki - *http://www.forensicswiki.org/wiki/Hachoir*
- Mercurial – *http://mercurial.selenic.com/wiki/*
- Plone4artist – *http://plone.org/products/plone4artistsvideo/*
- Django-massmedia - *http://opensource.washingtontimes.com/projects/django-massmedia/*
- GNU libextractor – *http://www.gnu.org/software/libextractor/*
- Amplee – *http://trac.defuze.org/wiki/amplee*
- Pyrenamer - *http://www.infinicode.org/code/pyrenamer/*
- Python Cryptography Toolkit – *http://www.amk.ca/python/code/crypto.html*
- Documentación del formato de archivo AVI – *http://www.alexander-noe.com/video/documentation/avi.pdf*
- Formato de Intercambio de archivo JPEG – *http://www.jpeg.org/public/jfif.pdf*

Maemo 5: La apuesta de Nokia por el Software Libre...

Hasta hace poco tiempo, tener completamente integrado el SO del pingüino en un dispositivo portátil (teléfono móvil, pda, etc.) era algo que requería bastante esfuerzo y en gran parte de los casos, por no decir la mayoría, era impensable. Actualmente encontramos varios intentos en el mercado de querer integrar de manera eficiente el SO Linux en este tipo de dispositivos. Pero, si deseamos tener integrado en un solo dispositivo una cámara, un GPS, teclado "qwerty", acelerómetros, teléfono móvil, e Internet gestionados por Linux de manera eficiente, solamente podemos pensar en el binomio Maemo + Nokia.



es@lpmagazine.org

Nokia comenzó la comercialización de sus *internet tablet* en 2005 con el lanzamiento del Nokia 770 utilizando la primera versión de Maemo la cual fue evolucionando hasta la versión 5 la cual incorpora un rediseño de la interfaz gráfica táctil entre todas sus mejoras y da vida al N900 de la compañía finlandesa.

Maemo 5

Maemo 5 es una plataforma de desarrollo basada mayoritariamente en código fuente abierto así como algunos componentes propietarios. Ha sido desarrollado por Nokia en colaboración con otros proyectos Open Source tales como el Kernel de Linux, Debian y Gnome entre otros.

El Sistema Operativo Maemo está basado en Debian GNU/Linux (*http://www.debian.org/index.en.html*) fue diseñado con la intención de optimizar el rendimiento en dispositivos con recursos limitados, así como el diseño de nuevas características para mejorar la visualización en pantallas pequeñas, rendimiento de la batería, y múltiples métodos de entrada entre otra características. La ultima versión estable es la 3.2010.02-8 – PR1.1.1.

Una de las más importantes características a resaltar es la interfaz gráfica de usuario "Hildon", la cual fue diseñada por Nokia para proveer una amplia funcionalidad en dispositivos móviles, además de integrar de manera eficiente las funcionalidades básicas de un sistema de escritorio (navegador, panel de control, barra de estado, etc.). Hildon está basado en GTK+ y forma parte del proyecto GNOME. En la Figura 1 se muestran los principales proyectos relacionados con Maemo. Existe una comunidad de Maemo en Internet la cual tiene el objetivo de desarrollar aplicaciones en torno a la plataforma Maemo. Actualmente tiene más de 22000 miembros registrados que contribuyen en más de 900 proyectos de desarrollo (*http://maemo.org/intro*).

La comunidad tiene un amplio número de herramientas y servicios para facilitar el proceso de desarrollo y mantenerse en línea con las necesidades de la comunidad.

¿Qué puede hacer Maemo?

La plataforma Maemo proporciona soporte para el desarrollo dirigido a las más importantes categorías tecnológicas requeridas por dispositivos móviles. Los componentes más importantes para cada categoría se mencionan en la Tabla 1.

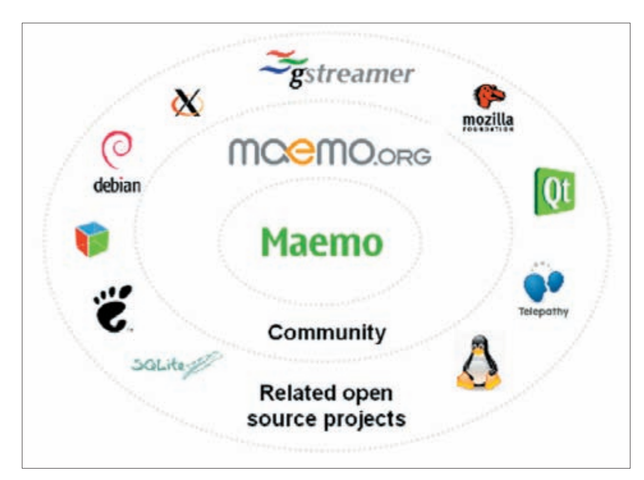


Figura 1. Proyectos Open Source relacionados con Maemo

Múltiples escritorios

Al igual que en cualquier ordenador con Linux, Maemo puede gestionar varios escritorios personalizados, agrupando aplicaciones en cada uno de ellos según las necesidades del usuario. Por defecto tiene activados 4 escritorios los cuales pueden ser desactivados a criterio, aunque nunca falta aquel usuario que requiere más de 4 escritorios y tendrá que hacer más ajustes de los necesarios para poder lograrlo.

Al ser un sistema táctil con solamente deslizar el dedo sobre la pantalla de izquierda a derecha o viceversa se realiza el cambio de escritorio. En cada escritorio se pueden agregar una gran cantidad de aplicaciones como el calendario, el reproductor multimedia, accesos directos a contactos, agenda, favoritos de Internet, mapas.

En la Figura 2 se muestran diferentes configuraciones de los escritorios.

Multitasking

Al igual que en nuestro ordenador de escritorio, Maemo puede gestionar varias aplicaciones a la vez con la estabilidad que solamente un sistema tipo GNU/Linux nos puede ofrecer. Esta es una de las grandes ventajas frente al teléfono de la manzanita el cual no soporta por defecto las aplicaciones multitarea, para optimizar el rendimiento gráfico. De igual manera que en un sistema de escritorio es factible visualizar las aplicaciones en ejecución, y terminar el proceso con aquella que diese algún problema.

Tabla 1. Software proporcionado por Maemo

Categorías	Aplicaciones
Multimedia	Desarrollo avanzado de aplicaciones multimedia con el uso de Gstreamer, V4L2 y Pulse Audio.
Gráficos	Soporte de Open GL ES 2.0 que permite el desarrollo de interfaces gráficas complejas, aplicaciones 3-D, juegos, etc.
Desarrollo de Aplicaciones	Maemo tiene la opción de dos sistemas de desarrollo (Hildon GTK+, Qt) que incrementan las opciones para los desarrolladores para crear o agregar nuevos proyectos.
Conectividad	Soporte de Bluez, Wlan, GW Obex, HSPA, etc.
Comunicaciones	Telepathy, Farsight, libnice, gUPnP, etc.



Figura 2. Personalización de escritorios con accesos a aplicaciones, Internet, contactos, agenda, diferentes widgets, etc.

Administrador de aplicaciones

Al igual que una distribución tipo Debian tiene un gestor de paquetes desde el cual podremos instalar una gran variedad de programas para aumentar nuestra experiencia con el SO. Cuenta con 7 repositorios por defecto y se le pueden activar otras tantas fuentes. Existen los repositorios de desarrollo y testeo (extras-testing y extras-devel), los cuales sólo son recomendables si se tiene conocimiento de sobra y no existe temor en tener que flashear el dispositivo si algo sale mal.

Actualizaciones del software

De igual manera las actualizaciones existentes se muestran de manera automática y uno decide en qué momento aplicar dicha actualización. Es altamente recomendable no hacer ningún tipo de actualización con los repositorios extras-devel y extras-testing, ya que se actualizarían algunos paquetes que podrían dar problemas muy serios en la configuración del sistema.

Internet

Maemo trae por defecto un navegador de Internet llamado MicroB basado en el motor de navegación de Mozilla, el cual ofrece una experiencia de navegación por Internet casi similar a dispositivos de escritorio. Es muy intuitivo en su manejo y cuenta con soporte total de Adobe Flash ™ 9.4, por lo que se pueden ver directamente páginas como Youtube o Google Maps entre otras. Una de las características que hacen la navegación más placentera es el control de zoom de la pantalla el cual puede ser de tres maneras: a) mediante los botones físicos del volumen, b) pulsando rápidamente dos veces sobre el área que se desea agrandar y c) dibujando un círculo en sentido de las manecillas del reloj para aumentar el zoom, y en sentido inverso para disminuir el detalle.



Figura 3. Administrador de tareas ejecutando 12 ventanas



Figura 4. Interfaz gráfica del Administrador de aplicaciones

Actualmente existe la versión nativa de Firefox para Maemo, pero al momento de la elaboración de este documento no se puso a prueba.

Aplicaciones de oficina

Por defecto Maemo no trae una suite completa de ofimática, únicamente tiene a disposición del usuario el visualizador de Office, "Documents to Go", el cual es una versión demo por 30 días.

Sin embargo, es posible tener OpenOffice.org, GIMP o AbiWord entre otras aplicaciones mediante la instalación de la imagen de Easy_Debian (*http://wiki.maemo.org/Easy_Debian/*) la cual es una instalación completa de Debian para poder ejecutar aplicaciones dentro de Maemo.

Para que la aplicación quede redirigida a un acceso al escritorio se tiene que hacer un archivo similar al de la siguiente tabla el cual se guarda con extensión ".desktop" y se almacena en */home/usr/.local/share/applications/hildon.*

Para el caso del icono de GIMP se sustituye el valor de "*debbie ooffice -writer*" por "*debbie gimp*".

Ademas cuenta con un potente editor de código, PyGTKEditor, el cual permite escribir en una gran variedad de lenguajes.

Multimedia

El sistema reproductor multimedia es muy completo, reproduce los formatos musicales más comunes(mp3, ogg, wma, acc) así como vídeo (wmv, mp4 y avi), y tiene un gestor de estaciones de radio por Internet. En el caso de las listas de reproducción están alojadas en */home/user/.mafw-playlists/* y pueden ser visualizadas o editadas con PyGTKEditor por citar un editor.

Listado 1. Ejemplo de acceso directo a OpenOffice.org Writer

```
[Desktop Entry]
Encoding=UTF-8
Name=OpenOffice Writer
Comment=openoffice
GenericName=text editor
Exec=debbie ooffice -writer
Terminal=false
X-MultipleArgs=false
Type=Application
Icon=ooo-writer
Categories=office;
```



Figura 5. MicroB desplegando un vídeo en Youtube y Google Maps

Gestor de Imágenes

Con la aplicación integrada se pueden visualizar las imágenes como miniatura en una cuadrícula o verlas completas por separado. Se pueden ampliar, desplazarse, editarlas y compartirlas.

El sistema cuenta con un sistema gestor para compartir archivos a través de servicios web tales como: Flickr, Ovi, Facebook, Youtube y Blogger. Este sistema es de fácil manejo permitiendo agregar etiquetas personalizadas a los archivos a compartir así como geolocali-

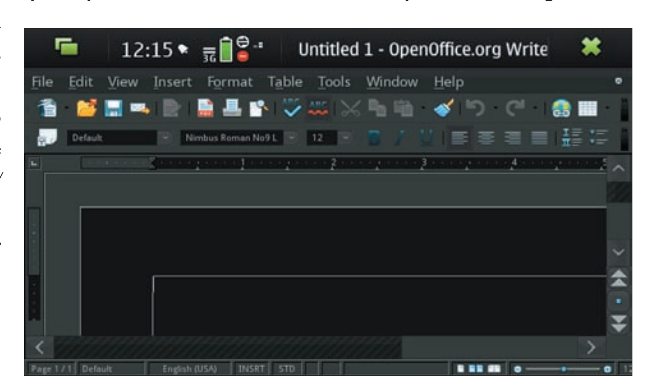


Figura 6. OpenOffice.org ejecutándose en Maemo 5



Figura 7. Iconos de OpenOffice.org y The GIMP en el escritorio

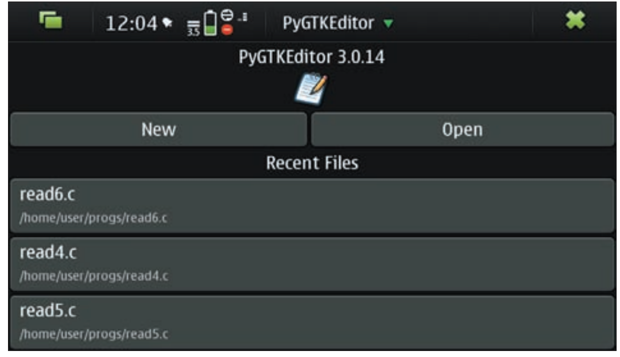


Figura 8. Editor de código PyGTKEditor

zación. Existe una aplicación demo llamada QuickPanorama que nos permite tomar panorámicas con solo desplazar la cámara en el sentido deseado. En la Figura 9 se muestra un ejemplo de ello.

Integración de contactos y teléfono

Uno de los grandes aciertos de este sistema es la integración de toda la información de nuestros contactos, la cual puede ser manual o semiautomática obteniendo información de sitios como Facebook. Además trae completamente integrado Skype para poder realizar llamadas por Internet.

Al tener toda la información de los contactos actualizada permite una gestión más eficiente, ya que al seleccionar un contacto se obtiene toda su información disponible como cuenta de msn, skype, facebook, yahoo, móvil, domicilio y cumpleaños por citar algunos ejemplos. Cabe mencionar que en ocasiones es necesario modificar la primera vez aquellos contactos que tienen cuenta en hotmail ya que es necesario copiar la etiqueta de la cuenta de msn a la base de datos de correo electrónico del dispositivo, y así al ejecutar la aplicación de correo electrónico aparezca la cuenta de msn en la opción de seleccionar destinatario.

Conectividad

Con Maemo es posible gestionar la conexión a Internet mediante banda ancha 3G, 2G o por WLAN. Lamentablemente hasta la ultima revisión de software todavía no contaba con soporte a redes "eduroam" que tengan el protocolo de seguridad EAP-TTLS+PAP y sigue en la lista de espera de los Bugs (*http://bugs.maemo.org/show_bug.cgi?id=1635*). Mencionan que en la próxima actualización mayor es muy probable que corrijan este fallo que nos afecta principalmente a los usuarios de redes académicas (será de esperar). El uso como módem, es completamente satisfactorio sin que se tenga queja alguna.

Calendario

El gestor de calendario tiene como principal ventaja el que permite sincronizar el calendario del dispositivo con el calendario de Gmail mediante Mail for Exchange permitiendo tener diferentes calendarios según las actividades del usuario.



Figura 9. Gestor multimedia

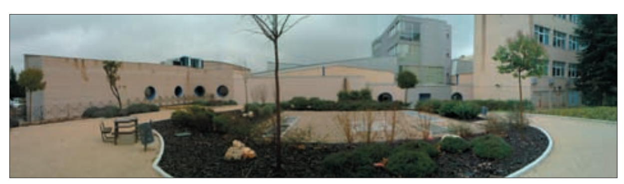


Figura 10. Foto panorámica

Al abrir la aplicación del calendario la primera vista es la agenda de actividades, pero desde el menú se puede seleccionar el tipo de vista ya sea semanal o mensual. Existe a su vez un widget que puede visualizar las actividades pendientes del calendario en el escritorio.

Mapas

Comparando esta versión de Maps con la última versión liberada para dispositivos Symbian, se queda corta, no dejando de ser funcional en gran medida. Se espera que en la nueva actualización mayor de software se mejore en gran medida la aplicación nativa de mapas de Nokia.

Por citar alguno de los puntos fuertes de esta versión de Mapas se puede mencionar:

- Cálculo de ruta entre puntos (con un buen nivel de aceptación),
- Agilidad en el desplazamiento del mapa,
- Bajo tiempo de adquisición de la señal de los satélites (usando A-GPS),
- Interfaz de usuario de fácil uso con los dedos.

Correo Electrónico

El gestor de correo electrónico es uno de los grandes aciertos, ya que tanto la configuración como el manejo de la aplicación es muy intuitiva lo que hace del envío y recepción de correos electrónicos una tarea agradable. Para realizar la correcta configuración de las cuentas de correo es necesario seguir los siguientes pasos:

- Seleccionar desde el menú de aplicaciones la aplicación *Correo-e,*
- Desde el menú seleccionar Nueva cuenta,
- Ingresar los datos referentes a la Región, proveedor del servicio, nombre de la cuenta, nombre, nombre del usuario, contraseña y dirección correo electrónico; en caso de seleccionar alguna cuenta que requiera configuración personalizada se ingresará el tipo de cuenta (IMAP4 o POP3), servidor entrante, etc.

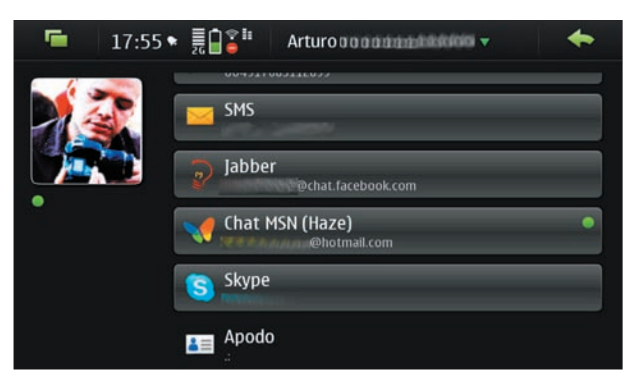


Figura 11. Integración total de la información de los contactos



Figura 12. Conectividad

Lamentablemente si se pretende descargar algún archivo adjunto que no reconoce la aplicación, simplemente no se podrá descargar. Pero, no hay problema, ya que abriendo una página web convencional se puede acceder a la pagina directamente del correo y descargar todos los archivos adjuntos que den problemas en la aplicación nativa.

X Terminal

Finalmente es necesario hablar de la consola terminal, la cual nunca debería de faltar en cualquier distribución de Linux. En el caso de Maemo utiliza la BusyBox y como con cualquier terminal de Linux se pueden hacer maravillas o crear un desastre, así que esta sección queda a la curiosidad innata del usuario de Linux por descubrir cada día nuevas aplicaciones y funciones que se pueden realizar mediante la consola.

Aunque.... no está por demás dar algún truco para el inicio.

Lo primero de todo es adquirir los super poderes de root, para lo cual desde el gestor de aplicaciones se instalará el programa “rootsh” el cual activará el acceso root mediante el comando “sudo gainroot”. A partir de ahí, podremos instalar, desinstalar, modificar, hackear y hacer un sin fin de cosas como conexiones ssh o monitorear la seguridad de redes WiFi con aircrack-ng (*http://www.universosymbian.org/programas-para-maemo/64953-flepp-aircrack-ng-nokia-n900.html*) por citar algún ejemplo. Se recomienda de manera especial el consultar la página dedicada a Power Users de Maemo.org para tener más referencias de los alcances que tiene el SO (*http://wiki.maemo.org/Category:Power_users*). Finalmente si algo sale mal cuando se está experimentando con el SO, ya sea por ser demasiado aventurero o por falta de conocimientos, será necesario reinstalar el SO por completo, para lo cual no estaría demás dar una leída al siguiente tutorial: *http://wiki.maemo.org/Updating_the_tablet_firmware.*

Conclusiones

Es un sistema potente y bastante bien logrado para ser relativamente nuevo, muy buena integración de software-hardware aunque falta por



Figura 13. Vista principal del calendario y el menú de sincronización de calendarios



Figura 14. Gestor de mapas de Nokia (*http://maps.ovi.com*)

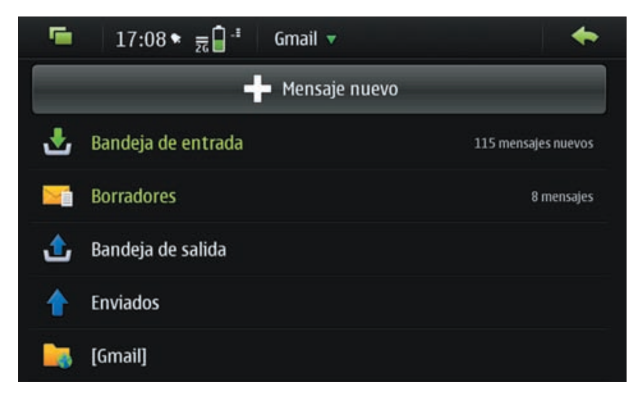


Figura 15. Gestor de Correo electrónico

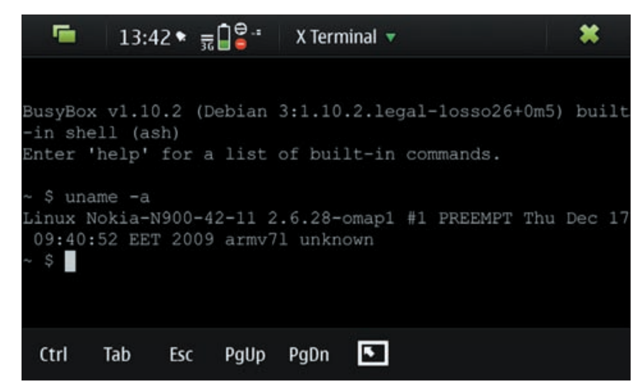
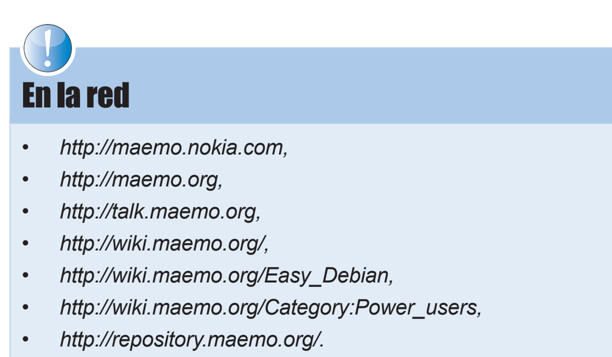


Figura 16. Terminal BusyBox mostrando la version del nucleo del kernel de Linux

el momento un catálogo más amplio de aplicaciones (estables) para sacar el máximo rendimiento al SO. Es posible que aquellos usuarios que migren de Symbian u otros SO extrañen algunas funciones o aplicaciones pero será de esperar un poco para cubrir esas necesidades. No se puede comparar con el teléfono de la manzanita ya que ambos tienen objetivos distintos, el de la manzanita prefiere tener respuesta rápida en gráficos y multimedia, Nokia apuesta por dedicar recursos a la multitarea y poder disfrutar de gráficos y aplicaciones multimedia al tiempo que se descarga un correo electrónico, se navega por Internet, o incluso escribir un artículo como éste. En otras palabras Nokia apuesta por sustituir “casi” por completo un ordenador portátil con su nueva generación de “Internet Tablets” en mi caso lo he conseguido, he disminuido la carga de mi mochila en 2Kg aproximadamente entre ordenador, cables y demás accesorios, y redunda en un beneficio directo para mi espalda. Ahora puedo pasear tranquilamente por la ciudad sabiendo que en cualquier momento puedo escribir algo de código e incluso compilar pequeños programas, enviar correos, navegar por Internet, revisar documentos de Word, editarlos, leer ebooks; es como traer un Pentium II en mi bolsillo.



En la red

- *http://maemo.nokia.com,*
- *http://maemo.org,*
- *http://talk.maemo.org,*
- *http://wiki.maemo.org/,*
- *http://wiki.maemo.org/Easy_Debian,*
- *http://wiki.maemo.org/Category:Power_users,*
- *http://repository.maemo.org/.*

Flight Gear 2.0

No es mi costumbre volver a comentar juegos que ya hayan sido comentados en esta sección, pero tras un cambio tan importante en un juego tan popular dentro del Software Libre como Flight Gear creo conveniente hacerlo. En ocasiones también lo hago con juegos que son ramas nuevas de juegos ya comentados, pero este caso es distinto, es la misma rama y el mismo juego, pero lo novedoso es que acaba de lanzarse la versión 2.0 con muchas mejoras.

FlightGear es un simulador de vuelo multiplataforma (encontraréis versiones de él para GNU/Linux, Windows, Mac OS X , Solaris (sparc/x86) , sgi y FreeBSD), de código abierto y libre. A día de hoy es la alternativa más importante frente a los simuladores de vuelo comerciales. El nivel de detalle de sus gráficos y el realismo de la simulación es comparable al de los mejores simuladores comerciales, entre los que se encuentra Microsoft Flight Simulator X.



Figura 1. Flight Gear 2.0

Internamente hace uso de Open GL y sus inicios se remontan a 2004 cuando fue lanzada su primera versión. La motivación del grupo de desarrolladores que se encuentra detrás del proyecto para empezar un juego de este tipo era la insatisfacción con los simuladores de vuelo presentes en el momento. Aunque la calidad gráfica y física de los mismos era muy buena, no tenían la posibilidad de modificarlos (como cualquier otro software de este tipo) para incluir nuevos aviones, pistas, comportamientos... La mejor opción era el código libre. Las mejoras de esta nueva versión afectan a todo el juego de forma directa (de hecho ha habido nuevas versiones con el paso del tiempo, pero nunca se había dado el salto de las 1.x a las 2.x). Además de mejoras en los gráficos y el sonido, se han mejorado aspectos como el manejo de algunos puntos clave y la inclusión de otras características entre las que destacaría un nuevo sistema de nubes en 3D, mejoras en la iluminación (en todo tipo de escenarios y condiciones meteorológicas). También se permite la personalización de los escenarios y mapas en los que volamos, y se han incluido más modelos de aviones, completando de esta forma un catálogo que podríamos calificar de impresionante. Aparte, se han incluido más aeronaves disponibles. En resumen, uno de los mejores juegos de código abierto que podemos encontrar en la actualidad, totalmente reformado y puesto al día para conquistar a usuarios de todos los sistemas. En muchos de los Top de los mejores juegos de Software Libre lo encontraréis y más tras el lanzamiento de esta nueva versión 2.0.

http://www.flightgear.org/



Tremolous

El segundo juego que os traigo este mes se llama Tremolous y ha salido en más de un Top de los mejores juegos libres, así que os podéis hacer una idea de lo que nos ofrece. Es un juego de acción en primera persona con una ambientación futurista al estilo de Quake y Alien versus Predator. También tiene elementos propios de juego de estrategia en tiempo real. De hecho con este segundo comparte algo más, en Tremolous podemos elegir entre dos equipos: aliens o humanos. Los dos bandos pueden construir estructuras y bases. Mientras que los aliens nacen de huevos cada vez que mueren mientras que los humanos nacen de telenodos. La idea es construir bases para defender las estructuras de las mismas.

El objetivo final es, como en todos los juegos de este tipo, eliminar todos los componentes del equipo contrario, asegurándonos además, la destrucción de las bases y nodos o huevos de forma que



Figura 2. Tremolous

ningún nuevo elemento contrario pueda volver a nacer. En éste, además, existe la posibilidad de comprar mejores armas e instrumentos defensivos, en el caso de los hombres; o poder evolucionar hacia un ser más poderoso en el caso de los aliens. Para ello deberemos matar el mayor número de enemigos posible.

El desarrollo del juego se divide en tres etapas distintas. Se pasa de una etapa a otra conforme el número de muertes de un bando llega a un límite. El paso a la nueva etapa también conlleva nuevas armas y evoluciones de forma que es otra forma de aventajar al contrario. Existen instaladores preparados para los tres sistemas operativos más importantes: Linux, Windows y Mac OS X. En el momento de escribir estas líneas están disponibles la versión 1.1 estable y la 1.2 en beta. Antes del lanzamiento del motor gráfico Quake III como Software Libre, era necesario tener instalado éste en el equipo porque en realidad el proyecto nació como una modificación de Quake III Arena.

En definitiva, otro de los grandes juegos del Software Libre, con unos gráficos de mucha calidad y un sistema de juego al más puro estilo shoot'em'up que gracias a la inclusión de elementos como las compras y las evoluciones, nos ofrece algo diferente y más adictividad. El juego ha sido descargado de más de un millón de veces y ha ganado galardones por ser uno de los mejores Mod del año (un mod es una modificación de un juego original que en ocasiones, como en este caso, llega a independizarse completamente del juego raíz).

http://tremulous.net/



Introducción al desarrollo
de videojuegos con SDL.NET

Francisco Javier Carazo Gil

El desarrollo de videojuegos es siempre una actividad de gran interés para todos los aficionados a la programación. La mezcla de ocio y tecnología forman un gran aliciente para comenzar a introducirse en el mundo del desarrollo. Atrás quedaron los lenguajes de más bajo nivel como C, que a pesar de ser siempre necesarios y útiles, pueden resultar algo complejos para los principiantes. Tecnologías como Mono, basada en la especificación .NET de Microsoft, junto con la que quizás es la librería para desarrollo de videojuegos más utilizada en el Software Libre, SDL, son una mezcla muy apetecible para empezar a sumergirnos en este mundo.



es@lpmagazine.org

No es el primer artículo que escribo en esta revista dedicado al desarrollo en Mono y espero que tampoco sea el último. Mono es una tecnología más madura de lo que se suele creer y que en la actualidad se encuentra en pleno crecimiento. Aunque es un proyecto polémico por estar basado en una tecnología de Microsoft, cada día es más reconocido por la comunidad libre y de hecho a día de hoy es parte esencial del entorno de escritorio Gnome. Personalmente puedo decir que para mí .NET puede ser lo que mejor ha hecho Microsoft en años, por lo que la base creo sinceramente que es muy buena.

Hace ya más de un año también tuve el placer de escribir un artículo presentando una introducción al mundo del desarrollo de videojuegos con SDL. La Simple DirectMedia Layer, que es el nombre completo de la API, es una solución muy popular en el desarrollo de videojuegos libres. Junto con Allegro, otra API similar, son las dos plataformas más utilizadas en este sector. ¿Qué problema tiene SDL para un principiante? Pues básicamente que para hacer uso de la misma las aplicaciones que escribamos han de estar implementadas en C/C++ y para los más noveles en el mundo de la programación puede ser un problema.

¿Qué es SDL.NET? Es el *binding*, algo así como la versión de SDL para .NET. Por supuesto, también es compatible con Mono por lo que tenemos otra puerta abierta para el desarrollo de videojuegos. Las ventajas de utilizar estas tecnologías en lugar de las anteriormente mencionadas, SDL y C/C++, es que C# es un lenguaje orientado a objetos que da muchas facilidades al desarrollador y al elevar el nivel de abstracción, ha de estar menos pendiente de detalles técnicos. Como todo lenguaje interpretado, os recuerdo que .NET/Mono se ejecutan bajo un entorno que interpreta una especie de *bytecode* al igual que Java y que por lo tanto, pierde algo de rendimiento.

Sin embargo, a pesar de esto, creo que es una combinación de primer nivel para introducirnos en el mundo del desarrollo de videojuegos a la vez que conocemos dos tecnologías muy relevantes.

Antes de seguir, comentaros que el objetivo de este artículo no es profundizar en la utilización de SDL. En esta



misma revista un compañero trató la creación de interfaces gráficas de usuario con SDL y yo mismo hice un artículo introductorio a la programación de videojuegos con SDL hace ya unos meses. La intención es daros los pasos a seguir para el que ya sabe SDL, poder utilizar un lenguaje de más alto nivel como C# o directamente comenzar a aprender SDL sobre un lenguaje más amigable y con menos detalles técnicos que C.

Desgraciadamente, se trata de un proyecto descontinuado, la última versión vio la luz el día 1º de mayo de 2008, en concreto la 6.1, pero sigue siendo suficiente para todos los propósitos que os propongáis.

Preparación e instalación

Veamos cómo configurar el entorno de desarrollo MonoDevelop, la tecnología que utilizaremos, Mono, y el *binding* de SDL para la misma, SDL.NET.

Mono y MonoDevelop

En función de la distribución que utilicéis, las circunstancias particulares cambiarán, pero básicamente os comento dos alternativas que probablemente os sirvan prácticamente a todos.

Puesto que Gnome utiliza Mono en muchas de sus aplicaciones, si utilizáis este entorno de escritorio es muy posible que lo tengáis. Si no lo tenéis tendréis que seguir los pasos que detallamos a continuación.

La primera es dirigiros a vuestro gestor de paquetes y buscar los paquetes correspondientes. Como *monodevelop* (el nombre del paquete probablemente será el mismo), depende de Mono, si elegís éste se os seleccionarán los demás paquetes necesarios para desarrollar y ejecutar programas con Mono. Resumiendo, instalando MonoDevelop a través del paquete homónimo, tendréis todo preparado.

La segunda solución, la más larga, es instalar Mono compilando el código fuente. Necesitaremos tener instalados: el compilador de C (gcc), Bison y las librerías de desarrollo para glib. Descargaremos el código fuente desde la sección de descargas del Proyecto Mono (pondrá algo así como Mono el número de la versión seguido de “sources”). El proceso de instalación es el siguiente:

- Descomprimimos y desempaquetamos el código fuente, gráficamente o mediante la consola: *$ tar zxvf mono-X.XX.tar.gz*
- Configuramos los archivos para realizar el *make*: *$ ./configure --prefix=/opt/mono*
- Ejecutamos *make* para ejecutar el código fuente: *$ make*
- Finalmente instalamos: *$ sudo make install*

Una vez terminada la instalación deberemos configurar debidamente las variables de entorno. Para ello ejecutamos desde la terminal el contenido del Listado 1.

Una vez ya tenemos instalado Mono, pasamos a instalar MonoDevelop de una forma análoga. Accedemos al sitio de MonoDevelop, descargamos el código fuente y:

- Desempaquetamos el código fuente y lo descomprimimos:
  `$ tar zxvf monodevelop-X.X.tar.bz2`
- Configuramos para crear el *make*:
  ``./configure --prefix=`pkg-config --variable=prefix mono` ``
- Compilamos: `$ make`
- Instalamos: `$ make install`

SDL.NET

Ya estamos preparados para instalar SDL.NET. En realidad no lo instalaremos sino que descargaremos el ensamblado que lo contiene y lo referenciaremos dentro de MonoDevelop. Accedemos a la web oficial de SDL dot NET (*http://cs-sdl.sourceforge.net/*) y en la sección de descargas elegimos la última versión del proyecto (nos redirigirá a la forja SourceForge). Dentro de las posibilidades que nos aparecen elegimos el fichero *.tar.gz* dentro del cual, en el directorio */bin* una vez descomprimido, tendremos el fichero *SdlDotNet.dll* y *Tao.Sdl.dll* que son los ensamblados que referenciaremos desde los proyectos.

Librerías SDL

Puesto que SDL.NET en realidad lo que se encarga es de gestionar las llamadas a las librerías de SDL deberemos instalar también éstas. Puesto que SDL es en realidad un gran conjunto de librerías que se reparten las funcionalidades, deberemos instalar las librerías que vayamos a utilizar en nuestros programas. Os recomiendo instalar por lo menos las siguientes:

- `libSDL-image`: encargada de manejar las imágenes.
- `libSDL-ttf`: escritura de letras de cualquier tipo TTF en nuestros programas.
- `libSDL-mixer`: reproducción de sonidos.
- `libSDL-net`: comunicación por la red.
- `libSDL-sound`: también relacionada con la reproducción de sonidos.

Además también deberemos instalar los paquetes relacionados con TAO (un framework que le permite a Mono interrelacionarse con SDL y Open GL):



Figura 1. Logo SDL



Figura 2. Logo .NET

- `libtaoframework-sdl1.2-cil`
- `libtaoframework-opengl3.0-cil`

Todos estos paquetes los encontraréis en vuestro gestor de paquetes o sino, deberéis buscarlos, compilarlos e instalarlos desde la red.

Desarrollo

Veamos a partir de ahora una serie de ejemplos de uso de SDL.NET en los que contrastar las diferencias con el desarrollo de SDL sobre C. Trabajaremos directamente sobre Mono Develop, obviando la compilación desde la terminal para centrarnos en lo que nos importa sobre el *port* de SDL.

Listado 1. Configuración variables de entorno

```
$ export PATH=$PATH:/opt/mono/bin
$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/mono/lib
$ export PKG_CONFIG_PATH=$PKG_CONFIG_PATH:/opt/mono/lib/pkgconfig
$ export MONO_PATH=/opt/mono/lib
```

Listado 2. Código fuente de Hola Mundo sobre SDL.NET

```
using System; // incluimos System
using SdlDotNet.Core; // y dos partes del SdlDotNet: el núcleo
using SdlDotNet.Graphics; // y los gráficos

namespace holaMundoSDL // espacio de nombres
{
        public class HolaMundo
    {
        [STAThread]
        public static void Main()
        {
            HolaMundo aplicacion = new HolaMundo();
            aplicacion.Iniciar();
        }

        public HolaMundo() // constructor
        {
            Video.SetVideoMode(640, 480);
            Video.WindowCaption = "¡Hola Mundo!";
        }

        public void Iniciar()
        {
            Events.Quit += new EventHandler<QuitEventArgs>(this.Salir); // evento de salida
            Events.Run();
        }

        private void Salir(object sender, QuitEventArgs e) // función que se ejecuta en el evento de salida
        {
            Events.QuitApplication();
        }
    }
}
```



Mi experiencia me dice que las versiones actuales de SDL.NET no tienen problema ninguno en compilarse sobre máquinas y librerías con juegos de instrucciones de 64 bits. El problema viene a la hora de ejecutar. Como en realidad SDL.NET lo que hace son llamadas a procesos a bajo nivel, las verdaderas SDL, en caso de que estemos trabajando con SDL a 64 bits tendremos graves problemas. Tantos que será imposible ejecutar ningún programa con más complejidad que el "Hola Mundo", que por cierto, sí funciona en estas circunstancias.

Aunque parezca erróneo lo que comento por el hecho de tratarse de Mono, una plataforma independiente del nivel hardware, SDL.NET interactúa con las DLL que están preparadas para recibir datos y órdenes de un tamaño y da errores y excepciones cuando trabajamos con DLL de 64 bits. SDL.NET es independiente de la plataforma como toda la implementación de .NET/Mono y por eso mismo el error se produce en ejecución y no en compilación.

Hola Mundo

Para crear nuestro primer programa con SDL.NET nos dirigiremos a Mono Develop, le indicaremos que queremos crear un nuevo proyecto. Elegiremos el proyecto para consola (no porque sea para consola sino para que incluya los elementos básicos y no incorpore referencias a GTK#) y en la pantalla de elegir "Funcionalidades del proyecto" no elegiremos ninguna (estas opciones pueden haceros falta si queréis desarrollar programas de producción para poder publicarlos, pero por ahora no nos son necesarios).

Lo primero que haremos será incluir los ensamblados en nuestro proyecto. Para ello, en la parte izquierda de la pantalla donde vienen los ficheros y clases del proyecto, hacemos clic derecho sobre "Editar referencias..." y en la pestaña "Ensamblado .Net" buscamos las dos *dll*: *SdlDotNet.dll* y *Tao.Sdl.dll* en el directorio donde las tengamos guardadas (podéis pasarlas al directorio propio de cada proyecto para mayor facilidad) y le damos a "Añadir". Para este ejemplo, en realidad sólo necesitaremos el primer ensamblado, pero incluyo los dos por si en un futuro hacen falta.

¿Qué va a hacer nuestro ejemplo? Vamos a lanzar una ventana con el título "¡Hola Mundo!" a una resolución de 640x480 píxeles.

Puesto que C# es un lenguaje orientado a objetos deberemos crear una clase HolaMundo que sea la que se encargue de esta labor. Definiremos los siguientes métodos:

- Constructor: creará la ventana indicando la resolución y el título de la misma.
- Iniciar: añadirá el evento salida de la aplicación que lo unirá al método salir.
- Salir: saldrá de la aplicación.

Con todo esto ya estamos en disposición de mostrar el código. Utilizaremos el atributo [STAThread] propio de .NET/Mono para indicarle a la máquina que la aplicación ejecutará sobre un hilo único. En caso de no indicarlo explícitamente podemos tener problemas con ciertos componentes que tienen o usan hilos. Indico algunos aspectos relevantes más sobre el código (ver Listado 2).

Tras ver este primer ejemplo ya podemos comentar diferencias y mejoras respecto de SDL.

- Como podéis apreciar, el hecho de trabajar con clases hace mucho más legible el código y accesible para los menos expertos.
- Nos alejamos de las cuestiones más técnicas, de los punteros y de las comprobaciones continuas acerca de si las funciones se han ejecutado correctamente. Ahora para este tipo de labores podemos manejar excepciones.
- El manejo de eventos es mucho más limpio.

Héroe

Se trata del siguiente ejemplo que vamos a desarrollar. La idea original es propia de los creadores de SDL.NET y de hecho incluso el *sprite* (el conjunto de imágenes para simular el movimiento del personaje) que uso son los del juego de ejemplos que trae SDL.NET (tienen licencia GPL por lo que podéis utilizarlos sin ningún problema para aprender y podéis usarlos de base para proyectos mayores que por supuesto, también sean GPL).

La idea es tratar con un héroe animado que ande por nuestra pantalla, incluyendo además animación y orientación. Debemos manejar los siguientes conceptos:

Refresco del juego y evento que se encarga de hacerlo

Definiremos la cantidad de veces por segundo que se deba refrescar el juego, y en cada refresco se llamará a un evento que se ejecutará. En concreto la definición de ambas acciones será como sigue:

```
Events.Fps = 50;
Events.Tick += new EventHandler<TickEventArgs>
(eventoTick);
```

Figura 3. Logo Proyecto Mono

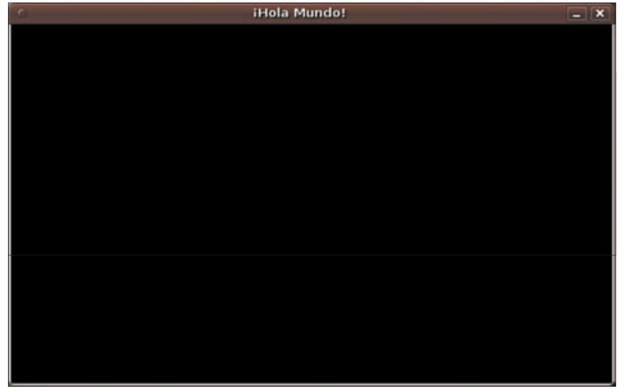


Figura 4. Resultado Hola Mundo

Declaración de eventos controladores de teclas pulsadas

Puesto que manejaremos el héroe con la cruceta del teclado, deberemos declarar eventos que manejen estas acciones, pulsa y liberar tecla:

```
Events.KeyboardDown += new EventHandler
   <KeyboardEventArgs>(eventoTeclaPulsada);
Events.KeyboardUp += new EventHandler
   <KeyboardEventArgs>(eventoTeclaLiberada);
```

Carga de la imagen

La manera más efectiva de cargar todas imágenes de golpe, es cargar un sólo fichero donde vengan las distintas imágenes que compongan la animación en forma de matriz y posteriormente dividirlo.

Lo primero que haremos por lo tanto será cargar el fichero "hero.png" que viene dentro del directorio "Data" de los ejemplos de SDL y lo incluiremos dentro de un nuevo directorio "Data" de nuestro proyecto. Para cargarlo manejaremos funciones propias de Mono/.NET y lo incluimos dentro de una instancia de superficie, *Surface* (Listado 3).

Creación de las colecciones de superficies y animaciones

Gracias a los siguientes métodos la creación de las animaciones es muy simple:

- Add de SurfaceCollection. Recibe tres parámetros:
  - Imagen: la que acabamos de cargar, en ella se encuentran todas las animaciones. Siempre deben de estar representadas por filas las distintas animaciones (andar arriba, andar abajo,...) siendo las columnas los distintos *frames* de la animación.
  - Tamaño del frame: variable de tipo Size con el tamaño, en nuestro caso 24x32.
  - Fila: entero que representa la fila dentro de la imagen donde se encuentran los *frames*. Pasándole este entero, SDL.NET ya recopila la secuencia completa.
- Add de AnimationCollection. Recibe dos parámetros:
  - Colección de superficies: la SurfaceCollection que acabamos de crear con los distintos *frames* de la animación.
  - Retraso: retraso existente en dos animaciones. Por defecto es 30.

Para "andar arriba" será cómo sigue. Las demás serán lo mismo pero cambiando la fila:

```
SurfaceCollection andarArriba = new
SurfaceCollection();
andarArriba.Add(imagen, new Size(24, 32), 0);
```

La creación de la animación sí es la misma en todos los casos:

```
AnimationCollection animacionArriba = new
AnimationCollection();
animacionArriba.Add(andarArriba, 35);
```

Elección del color para la transparencia del *sprite*

En SDL con SDL_SetColorKey y la máscara correspondiente elegimos qué color es el que debe de aparecer como transparente una vez cargado el *sprite*. Podéis ver en la Figura 5 el *sprite* del héroe que tiene el fondo de color magenta, para diferenciar lo que debe de ser transparente de lo que es en realidad el *sprite*. Esta técnica deja de tener sentido cuando existe la transparencia pero dado que ésta aporta un nivel de complejidad mayor a las imágenes, es válida y práctica en la mayoría de los casos.

Podemos ver, a continuación, lo simple de la elección de la transparencia en el siguiente código en comparación con el código equivalente en SDL:

```
heroe.TransparentColor = Color.Magenta;
heroe.Transparent = true;
```

Inicialización del *sprite*

Para inicializar el *sprite* llamaremos en el constructor si está animado (boolean), qué animación tiene en ese momento (Animation

Listado 3. Carga de la imagen

```
string ruta = Path.Combine("..", "..");
string directorio = "Data";
string nombreFichero = "hero.png";

if (File.Exists(nombreFichero))
{
        ruta = "";
        directorio = "";
}
else if (File.Exists(Path.Combine(directorio, nombreFichero)))
        ruta = "";

string fichero = Path.Combine(Path.Combine(ruta, directorio), nombreFichero);

Surface imagen = new Surface(fichero);
```



Listado 4a. Ejemplo héroe

```
using System;
using System.IO;
using System.Drawing;

using SdlDotNet;
using SdlDotNet.Graphics;
using SdlDotNet.Graphics.Sprites;
using SdlDotNet.Core;
using SdlDotNet.Input;

namespace ejemploHeroe
{
    public class EjemploHeroe
    {
        private AnimatedSprite heroe = new AnimatedSprite();
        private int velocidad = 2;

        [STAThread]
        public static void Main()
        {
            EjemploHeroe aplicacion = new EjemploHeroe();
            aplicacion.Iniciar();
        }

        public void Iniciar()
        {
            Events.Fps = 50;
            Events.Tick += new EventHandler<TickEventArgs>(eventoTick);
            Events.Quit += new EventHandler<QuitEventArgs>(eventoSalir);
            Events.KeyboardDown += new EventHandler<KeyboardEventArgs>(eventoTeclaPulsada);
            Events.KeyboardUp += new EventHandler<KeyboardEventArgs>(eventoTeclaLiberada);
            Events.Run();
        }

        public EjemploHeroe()
        {
            // Start up the window
            Video.WindowIcon();
            Video.WindowCaption = "Ejemplo heroe";
            Video.SetVideoMode(400, 300);

            string ruta = Path.Combine("..", "..");
            string directorio = "Data";
            string nombreFichero = "hero.png";

            if (File.Exists(nombreFichero))
```

Listado 4b. Ejemplo héroe

```
        {
            ruta = "";
            directorio = "";
        }
        else if (File.Exists(Path.Combine(directorio, nombreFichero)))
             ruta = "";

        string fichero = Path.Combine(Path.Combine(ruta, directorio), nombreFichero);

        Surface imagen = new Surface(fichero);

        SurfaceCollection andarArriba = new SurfaceCollection();
        andarArriba.Add(imagen, new Size(24, 32), 0);
        SurfaceCollection andarDerecha = new SurfaceCollection();
        andarDerecha.Add(imagen, new Size(24, 32), 1);
        SurfaceCollection andarAbajo = new SurfaceCollection();
        andarAbajo.Add(imagen, new Size(24, 32), 2);
        SurfaceCollection andarIzquierda = new SurfaceCollection();
        andarIzquierda.Add(imagen, new Size(24, 32), 3);

        AnimationCollection animacionArriba = new AnimationCollection();
        animacionArriba.Add(andarArriba, 35);
        heroe.Animations.Add("AndarArriba", animacionArriba);
        AnimationCollection animacionDerecha = new AnimationCollection();
        animacionDerecha.Add(andarDerecha, 35);
        heroe.Animations.Add("AndarDerecha", animacionDerecha);
        AnimationCollection animacionAbajo = new AnimationCollection();
        animacionAbajo.Add(andarAbajo, 35);
        heroe.Animations.Add("AndarAbajo", animacionAbajo);
        AnimationCollection animacionIzquierda = new AnimationCollection();
        animacionIzquierda.Add(andarIzquierda, 35);
        heroe.Animations.Add("AndarIzquierda", animacionIzquierda);

        // elegimos el color que se volverá transparente para el sprite
        heroe.TransparentColor = Color.Magenta;
        heroe.Transparent = true;

        // comenzamos la animación
        heroe.CurrentAnimation = "AndarAbajo";
        heroe.Animate = false;
        // situamos el sprite en mitad de la pantalla
        heroe.Center = new Point(Video.Screen.Width / 2, Video.Screen.Height / 2);
    }

    private void eventoTick(object sender, TickEventArgs e)
    {
```



Listado 4c. Ejemplo héroe

```
        // cada tick, 50 veces por segundo, se limpiará la pantalla y se colocará de nuevo el sprite
        Video.Screen.Fill(Color.Green);
        try
        {
            Video.Screen.Blit(heroe);
        }
        catch (System.ArgumentOutOfRangeException ex)
        {
            Console.WriteLine(ex.StackTrace.ToString());
        }
        Video.Screen.Update();

        // si el héroe está animado, elegimos la animación
        if (heroe.Animate)
        {
            switch (heroe.CurrentAnimation)
            {
                case "AndarIzquierda":
                    heroe.X -= this.velocidad;
                    break;
                case "AndarArriba":
                    heroe.Y -= this.velocidad;
                    break;
                case "AndarAbajo":
                    heroe.Y += this.velocidad;
                    break;
                case "AndarDerecha":
                    heroe.X += this.velocidad;
                    break;
            }
        }
    }

    private void eventoTeclaPulsada(object sender, KeyboardEventArgs e)
    {
        // vemos qué tecla se ha pulsado y en función de eso cambiamos la animación
        switch (e.Key)
        {
            case Key.LeftArrow:
                heroe.CurrentAnimation = "AndarIzquierda";
                heroe.Animate = true;
                break;
            case Key.RightArrow:
                heroe.CurrentAnimation = "AndarDerecha";
                heroe.Animate = true;
                break;
```

Listado 4d. Ejemplo héroe

```
                case Key.DownArrow:
                    heroe.CurrentAnimation = "AndarAbajo";
                    heroe.Animate = true;
                    break;
                case Key.UpArrow:
                    heroe.CurrentAnimation = "AndarArriba";
                    heroe.Animate = true;
                    break;

                case Key.Escape:
                case Key.Q:
                    Events.QuitApplication();
                    break;
            }
        }

        private void eventoTeclaLiberada(object sender, KeyboardEventArgs e)
        {
            // vemos qué tecla se ha levantado y actualizamos en consecuencia
            if (e.Key == Key.LeftArrow && heroe.CurrentAnimation == "AndarIzquierda")
                heroe.Animate = false;
            else if (e.Key == Key.UpArrow && heroe.CurrentAnimation == "AndarArriba")
                heroe.Animate = false;
            else if (e.Key == Key.DownArrow && heroe.CurrentAnimation == "AndarAbajo")
                heroe.Animate = false;
            else if (e.Key == Key.RightArrow && heroe.CurrentAnimation == "AndarDerecha")
                heroe.Animate = false;
        }

        private void eventoSalir(object sender, QuitEventArgs e)
        {
            Events.QuitApplication();
        }
    }
}
```

Collection), y posición del centro del *sprite* (Point). Éste último es mucho más cómodo que calcular el centro del mismo y luego posicionarlo en función a él, ya que SDL.NET lo hace por nosotros.

```
heroe.CurrentAnimation = "AndarAbajo";
heroe.Animate = false;
heroe.Center = new Point(Video.Screen.Width / 2,
Video.Screen.Height / 2);
```

Evento tick

¿Qué haremos en cada *frame* del juego? Al comienzo hemos indicado que el juego deberá refrescarse 50 veces por segundo y las acciones a ejecutar en cada refresco las definimos aquí. En nuestro caso:

- Rellenaremos la pantalla de color verde.
- Situaremos al héroe dentro de ella.
- La actualizaremos.
- En caso de que el héroe esté en movimiento, incrementamos su posición en función a la dirección que siga.

Dejo el código para mostrar de los eventos al final, con todo el conjunto, porque es muy legible y ocupa demasiado espacio para repetirlo dos veces, aquí y luego.

Eventos tecla pulsada y liberada

¿Qué haremos cuando el jugador pulse una de las teclas y luego la libere? Cuando la pulse, en función de la tecla, deberemos empezar a mover al muñeco en dicha dirección. Para desencadenar el movi-





Figura 5. Toma de pantalla del ejemplo del héroe

miento, deberemos activar la animación "andarArriba", "andarAbajo"... o la que toque. Esta propiedad será la que luego haga que el muñeco se mueva, ya que el movimiento en sí se maneja en el eventoTick. Al liberar la tecla, el *sprite* deberá pararse.

Controlamos ambos eventos con *Events.KeyboardDown* y *Events.KeyboardUp* que nos proporcionan una variable del tipo KeyboardEventArgs de donde podemos extraer la información referente a la tecla que está siendo pulsada.

Evento salir

Ídem que en el Hola Mundo.

Os dejo el código completo a continuación, con comentarios dentro del mismo (Listado 4) y una toma de pantalla del resultado (Figura 6).

Conclusiones

Aunque de manera muy breve, espero haberos presentado a lo largo de este artículo las líneas más importantes de lo que significa SDL.NET. El hecho de que se encuentre descontinuado o los problemas que puede tener a la hora de ejecutar sobre algunas arquitecturas, no le quitan la importancia a un proyecto que llegó a la versión 6.1 y que entre otras cosas que no hemos contado, puede tratar directamente con OpenGL.

Otro detalle de importancia que hemos pasado por alto hasta ahora es el hecho de la portabilidad. Al tratarse de código compilado para Mono/.NET, no existen problemas para ejecutarlo posteriormente sobre equipos Windows o Mac OS que tengan el *framework* de .NET

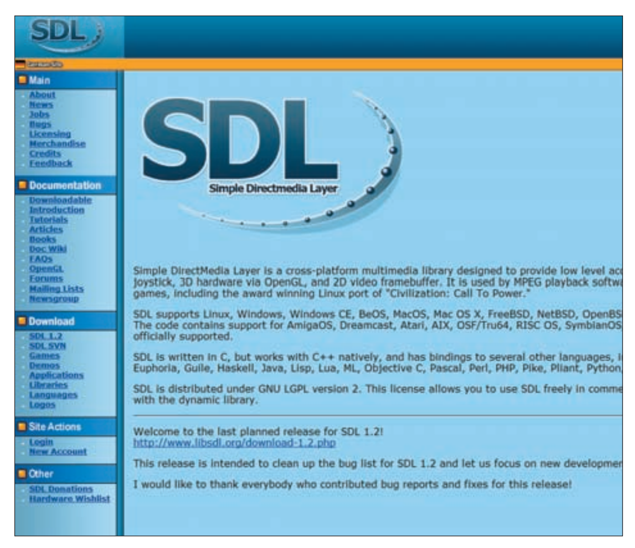


Figura 7. Proyecto SDL Website



Figura 6. Miguel de Icaza, fundador y mayor impulsor del Proyecto Mono

o de Mono instalado. Los programas con SDL sí requieren ser recompilados para cada máquina y plataforma donde vayan a ejecutarse.

Por otro lado, como habéis podido observar a través de los ejemplos, a pesar de seguir teniendo las dificultades técnicas que conllevan el desarrollo de videojuegos o de cualquier interfaz de este tipo, se simplifica mucho la parte técnica y se abstrae enormemente de las cuestiones más cercanas a la máquina. Es cierto que ésto no es lo ideal para tener un desarrollo muy eficiente, pero sí lo es para el aprendizaje.

Aún así no deja de ser un proyecto de reducidas dimensiones en el que no está basado ningún gran proyecto y que más que para aplicaciones de producción os lo recomiendo para iniciaros en el mundo del desarrollo de videojuegos y productos multimedia, y si no conocéis la plataforma Mono, puede ser un buen momento para probar con ella.



En la red

- SDL.NET – *http://cs-sdl.sourceforge.net/*
- Mono – *http://mono-project.com/*
- MonoDevelop – *http://monodevelop.com/*
- Mono Hispano – *http://www.mono-hispano.org/*
- SDL – *http://www.libsdl.org/*



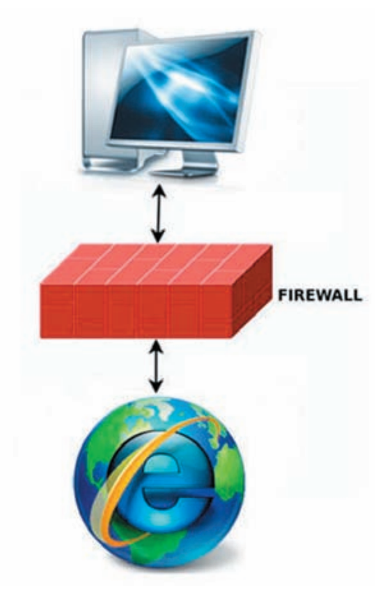
Sobre el autor

Francisco Javier Carazo Gil es Ingeniero Técnico en Informática de Sistemas. Nacido en Córdoba, actualmente está estudiando Ingeniería en Informática además de trabajar en el Consejo Superior de Investigaciones Científicas. Es webmaster de LinuxHispano.net, sitio del que es uno de los fundadores, además de ser el responsable de LinuxHispano-Juegos y colaborador habitual del podcast de LinuxHispano. En esta revista es colaborador habitual y sus intereses son principalmente el software libre, la programación y todo lo relacionado con GNU/Linux. Su sitio web personal está en *http://www.jcarazo.com*. Acaba de editar un libro para la editorial Ra-Ma de nombre: "Ubuntu Linux, instalación y configuraciones básica en equipos y servidores". Podéis contactar con él a través de *carazo@gmail.com*.

Endian Firewall:
un cortafuegos para todos los públicos

Isabel María Carrasco Martínez, Alfonso Vera Rubio

Endian Firewall es una distribución Linux para su uso específico como cortafuegos que proporciona una simple e intuitiva interfaz web de administración. Originalmente nació como un derivado de IPCop, actualmente se basa en Linux From Scratch. Tiene como objetivo ser un cortafuegos sencillo y con pocos requerimientos de hardware orientado a usuarios domésticos o a pequeñas empresas.



es@lpmagazine.org

Endian Firewall está capado y sólo tiene instaladas las herramientas justas para su función como firewall, limitando el daño que podría hacer un intruso que comprometiera el sistema. Permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a Internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

Las diferentes zonas las divide en colores, siendo:

- Roja = zona de Internet,
- Verde = Red de Área Local (LAN) cableada,
- Naranja = zona desmilitarizada (DMZ),
- Azul = Zona Inalámbrica (Wireless).

Endian Firewall incluye, entre sus características principales, una gran variedad de funciones "Out the Box":

- Firewall con inspección de estados,
- Antivirus HTTP/FTP.[1],
- Filtro de Contenido Web. [2],
- Antivirus POP3/SMTP, Anti-Phishing y Antispam,
- VPN SSL/TLS,
- IDS.[3],
- Alta Disponibilidad,
- NTP, DHCP,
- y mucho más ...

Con este artículo práctico repasaremos los aspectos más significativos, de la configuración de Endian como firewall de nuestra red, repasarlos todos nos llevaría un número de la revista. A la hora de decidirse a implementarlo no dude en consultar la documentación oficial del proyecto[4] y foro de usuarios[5] donde estarán encantados de ayudarle.

Topología de Red

La configuración de nuestro caso de estudio se realizará sobre una topología de red básica con una LAN en 192.168.0/24, una pequeña DMZ con un servidor web y uno de correo en 192.168.1./24 y la conexión a Internet en 192.168.2/24.

Nuestro cortafuegos tiene 3 interfaces de red una en cada una de las redes:

- Interfaz Roja
- Interfaz Verde,
- Interfaz Naranja.

El router de nuestro proveedor tiene asignada la IP 192.168.2.50 en la red Roja.

La configuración física de nuestra LAN se compone de:

- Un switch de 24 puertos para la LAN interna y la interfaz verde del cortafuegos,
- Un switch de 8 puertos para los servidores en DMZ y la interfaz naranja del firewall,
- Un switch de 4 puertos para conectar el router de nuestro proveedor de Internet y la interfaz roja de Endian.

Instalación Inicial

Una vez descargada la imagen (.iso) del sistema desde SourceForge[6], podemos comenzar la instalación: inserte el CD de instalación y arranque la computadora, se encontrará con "Anaconda", el instalador de Red Hat en modo texto, deberá responder a unas cuantas sencillas preguntas: la configuración del idioma, si queremos permitir el acceso vía puerto serie y la configuración de la interfaz verde (la que se encuentra en nuestra red). El particionado y la elección de paquetes lo realiza por nosotros, no tema.

Una vez terminada esta primera parte el sistema nos avisa que va a reiniciar y que podemos seguir la configuración conectándonos a la interfaz verde vía web. *https://192.168.0.100:10443*

Una vez reiniciada la máquina accedemos a la interfaz web y comenzamos con el proceso de configuración:

- Pulsamos en Siguiente y nos aparece la configuración del idioma y la zona horaria,
- Elegimos que no queremos restaurar una copia de seguridad ya que realizamos una instalación limpia,
- Damos de alta a los dos usuarios que necesitamos: admin para acceder vía web y root para acceder vía ssh a la máquina,
- Ahora configuramos la interfaz roja, una tarjeta de red con direccionamiento estático (que estará conectada al mismo switch que nuestro router),
- En este punto podemos añadir una interfaz naranja (DMZ) o una zona azul (Wireless) en nuestro caso seleccionamos una interfaz naranja,
- En este paso podemos reconfigurar la interfaz verde, revisar que la tenemos asignada a la ethernet correcta y darle un nombre a nuestro host,
- Ahora es el turno de asignar una dirección IP a la interfaz roja, asignarla a la tarjeta de red correcta y añadir una "puerta de enlace predeterminada" que será la interfaz privada de nuestro router,
- Los pasos finales solicitan los DNS de nuestro proveedor de Internet y la posibilidad de configurar el envío de correo al administrador.

¿Y ahora? Una vez instalado, desde una computadora en la zona verde, compruebe que la navegación está permitida, desde una consola intente conectar vía telnet con el puerto 389 (ldap) con ldap.fnmt.es para comprobar que no puede hacer consultas a directorios en Internet. Ese será nuestro próximo paso abrir puertos para el tráfico de salida desde nuestra red interna a Internet.

Tráfico saliente, de nuestra red a la inmensidad

Seleccione CORTAFUEGOS de la barra de menús en la parte superior de la pantalla, a continuación, haga clic en OUTGOING TRAFFIC en el menú de la izquierda de la pantalla. Endian Firewall ya viene preconfigurado con una serie de reglas, que permiten el tráfico de salida típico para acceder a Internet, desde la zona verde (Red Local) usando los servicios más comunes (HTTP, HTTPS, FTP, SMTP, POP, IMAP, POP3s, IMAPs, DNS, ping). El resto de servicios se bloquean por defecto.

En el caso de que tuviéramos zona azul (Wireless), tendríamos el acceso a HTTP, HTTPS, DNS y ping, en la zona NARANJA (DMZ) sólo tiene permitido por defecto el tráfico DNS y el ping. Todo lo demás está prohibido por defecto.

En este punto felicitamos a los desarrolladores de Endian, uno de sus rivales IPCop recién instalado permite el tráfico sin restricciones de la interfaz verde a la roja, o lo que es lo mismo, todo el tráfico saliente está permitido.

En esta sección se pueden desactivar y activar, editar o eliminar reglas haciendo clic en el icono apropiado (lápiz, papelera, etc.). También puede añadir sus propias reglas. Vamos a agregar una nueva regla pulsando en "add new rule" para poder consultar ldap en Internet (Puerto 389/tcp).

Para definir una regla necesitaremos los siguientes parámetros:

- Origen: una zona, interfaz o host, en nuestro caso la zona verde,
- Destino: la zona roja (Internet),

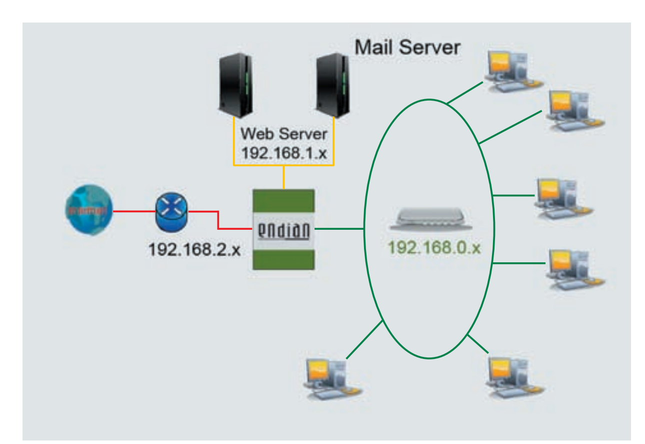
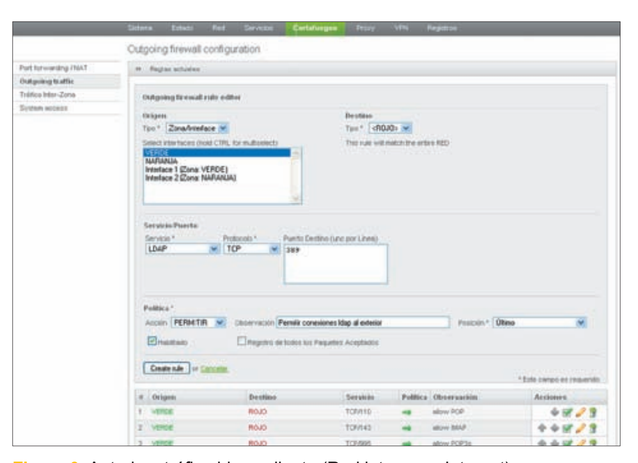


Figura 1. Topología de red para el caso de estudio



Figura 2. Configuración de interfaces de red


Figura 3. Autorizar tráfico ldap saliente (Red interna -> Internet)

- Puerto Destino: 389,
- Acción: permitir,
- Observación: protocolo ldap,
- Habilitar: checkbox marcado por defecto,
- Registro de los paquetes: para guardar un registro del tráfico ldap desde nuestra red a Internet.

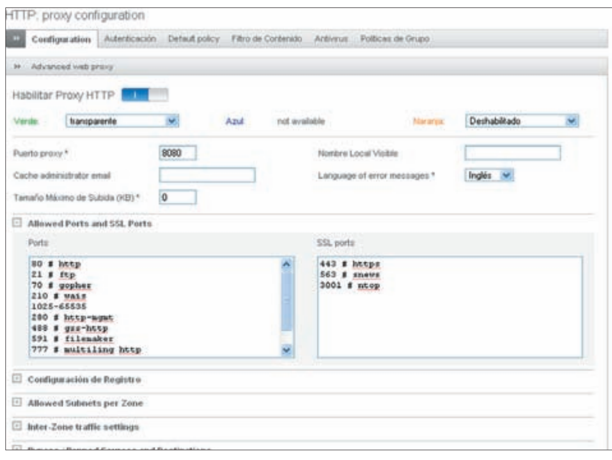
Una vez que manejamos el tráfico que sale de nuestra red hacia Internet estamos preparados para comenzar con NAT[7]: dirigir el tráfico que llega al puerto 80 de nuestra IP pública a nuestro servidor web situado en la Zona Naranja.

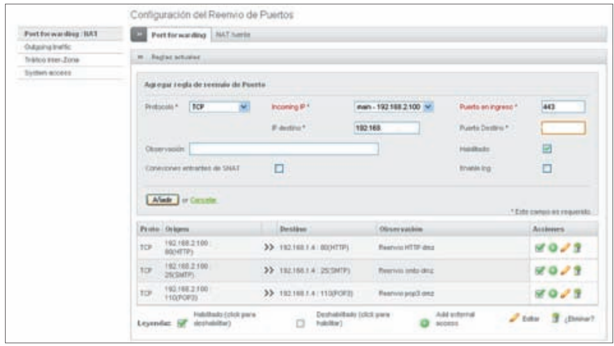
Reenvío de puertos, publicando nuestros servicios en Internet

Seleccione CORTAFUEGOS de la barra de menús en la parte superior de la pantalla, a continuación, seleccione Port Forwarding/NAT en el submenú en el lado izquierdo de la pantalla.

Esta opción se utiliza para restringir y/o redirigir el tráfico que llega a la Zona Roja (Internet) a los host en la Zona Naranja (DMZ) o incluso a la Zona Verde (LAN), aunque esto no es recomendable desde el punto de vista de la seguridad.

Ahora definiremos qué puerto de la interfaz roja será enviado a una pareja (host, puerto) en la zona Naranja. En nuestro caso queremos realizar NAT para que el puerto 80 (Web) de la interfaz roja sea reenviado al puerto 80 de nuestro servidor web en la DMZ, realizaremos después la misma operativa para el servicio SMTP (puerto 25) y el servidor de correo.


Figura 5. Configuración básica Proxy Web

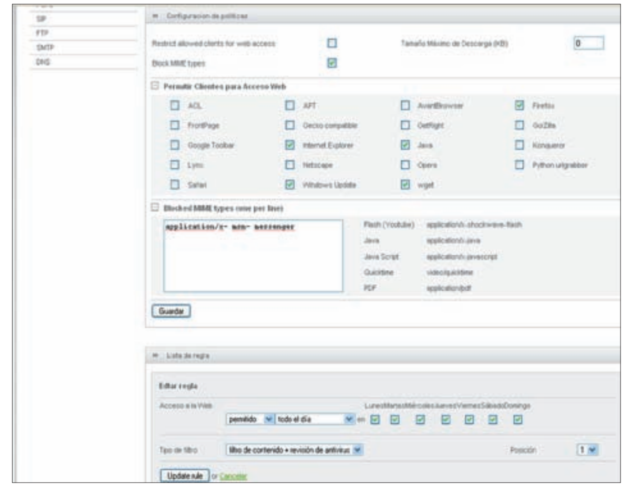

Figura 4. Publicando nuestros servicios en Internet

¡No se olvide de realizar NAT desde su router hasta la interfaz roja del firewall!

Necesitaremos los siguientes datos:

- Protocolo – TCP, UDP, GRE (usado para el establecimiento de túneles) o todos (TCP),
- IP de entrada (Incoming) - IP de la interfaz roja (192.168.2.100),
- Puerto en la IP de entrada: el puerto donde escuchar en la interfaz roja (80),
- IP Destino: la IP del host a la que reenviaremos el tráfico (192.168.1.4),
- Puerto de Destino: el puerto en el host de destino que recibirá el tráfico reenviado (en nuestro caso el 80),
- Observación – un pequeño comentario de la utilidad de la regla,
- Habilitar - checkbox para habilitar la regla (por defecto está marcado),
- Conexiones entrantes SNAT - (Nat en Origen) habilitaremos este checkbox si queremos que los paquetes que vengan del exterior parezcan procedentes de la interfaz roja del cortafuegos en lugar de la IP real,
- Enable log – chequearemos este enlace si queremos tener constancia de todas las conexiones que lleguen al puerto 80.

Hasta aquí hemos conseguido los primeros objetivos, controlar qué tráfico sale de nuestra red y publicar en Internet nuestros servidores de correo y Web. Ahora no debe de confiarse, por mucho que intente educar a sus usuarios para que eviten páginas potencialmente peligrosas, no le obedecerán. En la siguiente sección controlaremos la navegación para salvaguardar a nuestros usuarios.


Figura 6. Configuración de Políticas

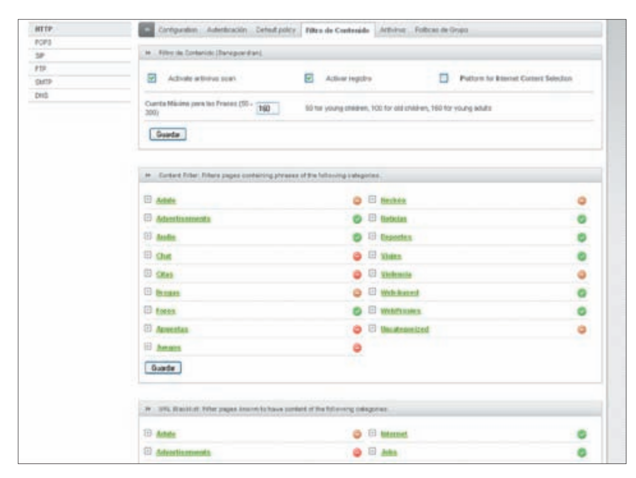


Figura 7. Configuración de Filtrado de contenido

Configuración de Proxy Web y Filtrado de Contenidos

Para acceder a los servicios de proxy y filtrado, como siempre, seleccione en la barra superior de la pantalla la opción PROXY. Un proxy es un servicio en nuestro cortafuegos que actúa como "guardián" entre los clientes (los navegadores de nuestra LAN) y distintos servicios de red, en nuestro caso la navegación Web. Los clientes se conectan al proxy que a su vez se conecta al servidor Web destino, el proxy es capaz de recuperar, filtrar e incluso bloquear la información de ese servicio Web para que no llegue a nuestros clientes. Un proxy es transparente cuando todo el tráfico pasa por él sin necesidad de ninguna configuración especial en el cliente, por tanto un proxy no transparente requiere configuración en el cliente (Navegador).

Ahora pasamos a destacar los servicios de proxy disponibles en Endian Firewall, pueden ser accedidos como siempre en el submenú de la izquierda:

- HTTP: configuración del proxy Web (Squid)[8], incluye autenticación, filtro de contenidos y antivirus,
- POP3: configuración del proxy con filtro antispam y antivirus,
- SIP: configuración del proxy SIP (Servicios de Voz sobre IP),
- FTP: habilitar o deshabilitar el proxy ftp, incluye chequeo antivirus,
- SMTP: configurar el proxy para enviar y recibir mensajes vía SMTP, incluye filtro antisamp y antivirus,
- DNS: configuración de un servidor de cache DNS incluyendo antispyware.

En nuestro caso sólo haremos uso del proxy y el filtrado Web, ya que nuestro servidor de correo realiza satisfactoriamente las funciones del filtrado POP3 y SMTP, en el caso de recibir correo desde cuentas externas dejamos como ejercicio al lector la configuración del filtrado de correo.

Para configurar el proxy http seleccione la opción PROXY en el menú principal y HTTP en el submenú de la izquierda.

Como primer paso arranque el proxy (pulsando el botón Habilitar Proxy Web), una vez hecho esto aparecerán nuevas opciones.

Ahora elegiremos de qué forma queremos que se comporte el proxy en nuestras zonas, en el caso de la zona verde, nos interesa usar el modo transparente y deshabilitarlo en la zona naranja.

El resto de opciones en la pestaña principal son los protocolos y puertos que pasarán por nuestro proxy, si registramos logs de acceso, las subredes de cada zona, si se realiza "bypass" sobre alguna IP en concreto de la red (no pasa por el proxy).

En la segunda pestaña de configuración del proxy AUTENTICACIÓN no es necesario realizar ninguna modificación ya que en principio no solicitaremos usuario y contraseña para los usuarios que navegan desde nuestra red. Si dispone de un servicio de Active Directory en su red puede conectar Endian con éste y permitir la navegación a determinados grupos de usuarios solamente.

La tercera pestaña en la configuración del proxy establecerá la política por defecto, utilizaremos las opciones por defecto fijando la política en filtro de contenidos y antivirus sin restricción horaria, en cualquier momento y haciendo uso de unos sencillos checks y desplegables puede establecer las restricciones horarias para la navegación y para la política por defecto. Podemos además bloquear distintos agentes (Explorer, Firefox, etc.), en este apartado también se encuentra el bloqueo por tipo mime, por ejemplo podríamos denegar la descarga de archivos ejecutables.

La siguiente pestaña nos ayudará de forma gráfica a gestionar el filtrado de contenidos mediante SquidGuard.

En la primera parte de la pantalla encontramos tres checkbox para activar el antivirus vía Web, el log de los contenidos y PICS[9], dejaremos sólo el último sin marcar.

Los dos siguientes paneles nos ayudarán a manejar de manera sencilla (con un icono de ok y uno de Stop) las webs permitidas o denegadas por el filtro de contenidos y por las listas negras. Como última parte tenemos unas cajas de texto donde incluir nuestras propias listas blancas y negras de URLs.

Sírvase un café y descanse, se lo ha ganado, ha pasado con éxito el ecuador de la prueba, casi tiene listo su cortafuegos.

Manejando conexiones seguras con OpenVPN

Seleccione VPN de la barra de menús en la parte superior de la pantalla para acceder a la configuración del servicio en su firewall. Las

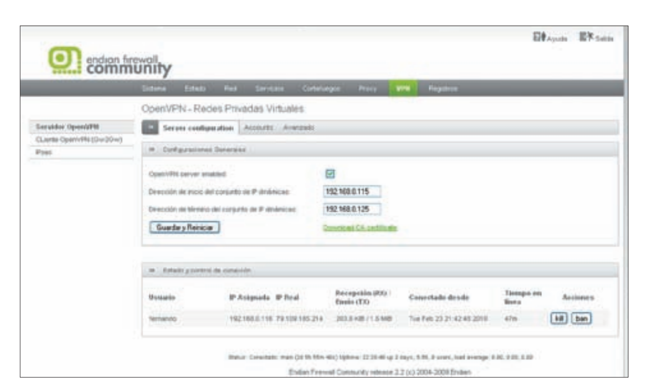


Figura 8. Configuración inicial servicio VPN

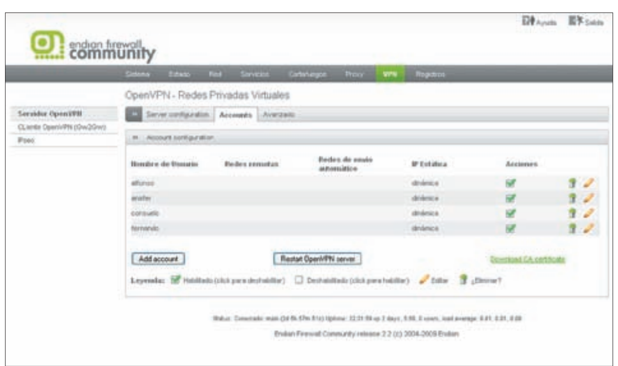


Figura 9. Añadiendo usuarios al servicio VPN

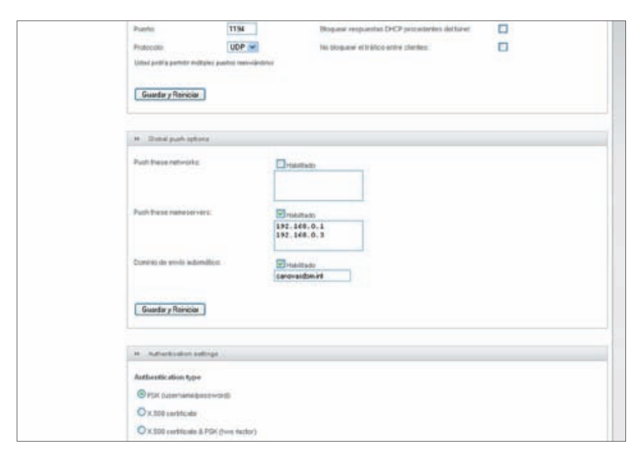


Figura 10. Configuración avanzada VPN

Redes Privadas Virtuales (VPN) permiten a dos redes locales conectar de manera segura a través de un contexto inseguro como es Internet. El tráfico de red a través de la conexión VPN se transmite de forma segura estableciendo un túnel cifrado, aislando su tráfico de miradas indiscretas. Existen dos tipos de conexiones: la primera uniendo dos redes (Gw2Gw) entre supongamos las dos sedes de su empresa que se encuentran en ciudades diferentes y una segunda configuración (RoadWarrior) donde los clientes son equipos de alguna parte de Internet que establecen el túnel VPN para conectarse a nuestra red de una manera segura. El ejemplo que detallamos a continuación se realizará sobre el segundo caso, configuraremos nuestra VPN para aceptar la conexión de clientes dispersos por Internet.

La configuración de una VPN Gw2Gw también la dejamos como ejercicio al lector (no íbamos a realizar todo el trabajo por usted)[10].

En la primera pestaña «configuración del servidor» activamos el servidor OpenVPN y definimos el rango de direcciones dentro de la zona verde que se va a asignar a la conexión de los clientes. Tenga



Figura 12. Endian Community

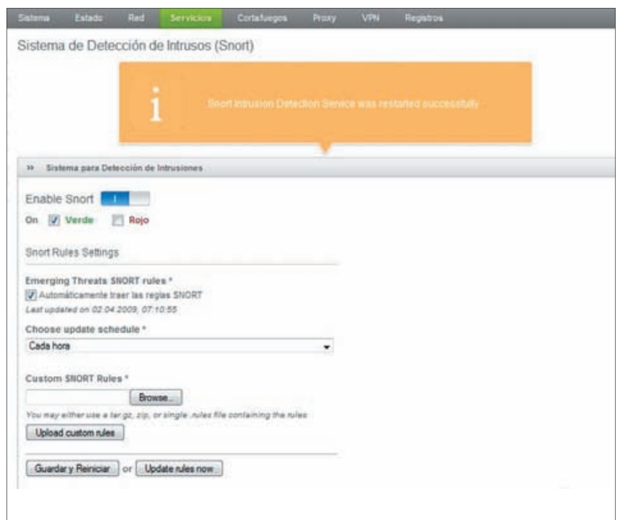


Figura 11. Configuración de Snort

en cuenta que todo el tráfico de ese pool de direcciones va a ser analizado por el firewall VPN y puede ser costoso, asigne un grupo de direcciones reducido.

Haga clic en guardar e inicie el servicio, la primera vez que éste se ejecuta genera un certificado para el servidor, descárguelo, lo necesitará más tarde para la configuración de los clientes. En el último panel de esta pantalla se muestra la lista de clientes conectados, desde aquí es posible desconectar a los usuarios y prohibirles la conexión después de haberlos desconectado, ¡es muy divertido!

El siguiente panel (Figura 9) es de configuración de cuentas para los usuarios. Para dar de alta una nueva cuenta de usuario necesitamos:

- Usuario: nombre de usuario,
- Contraseña: password de usuario.

En principio el resto de opciones de enrutado las dejamos por defecto, el resto de opciones las configuraremos en la siguiente pestaña: opciones avanzadas.

En esta ventana podremos modificar el puerto y el protocolo donde escuchará nuestro servicio, es recomendable dejarlo por defecto en el puerto 1194 y udp, aunque puede necesitar cambiarlo en el caso de que sus usuarios remotos se encuentren en una red desde donde solamente puedan usar ciertos puertos, es típico encontrar configuraciones en el puerto 443, https, para evitar las restricciones de la red origen. Las redes a las que tendrá acceso nuestro cliente, si no ponemos ninguna llegará sólo a la red local (Interfaz verde), en el caso de que necesitáramos que accediera a la DMZ añadiríamos 192.168.1/24.

Es necesario indicar los servidores DNS para que nuestros clientes puedan usar los DNS internos, asimismo si añadimos el sufijo dns, facilitaremos la vida de nuestros clientes.

En el panel final (Figura 10) podemos modificar la forma en la que se autenticará el usuario por contra nuestro servidor, para comenzar lo dejamos con usuario y contraseña, esta configuración es la más insegura pero la más cómoda para los "administradores noveles". Recomendamos el uso de certificados para la autenticación del usuario, desde esa misma pantalla podrá generar los ficheros pkcs12[11] para sus usuarios, incluso la doble autenticación: uso de claves + login y password.

Figura 13. Foro de soporte (en inglés)

Snort: Detectando patrones sospechosos

Endian Firewall nos provee de snort como sistema IDS (Intrusion Detection System).

El funcionamiento de los IDS es sencillo, se basan en el análisis del tráfico que compara con una base de firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes mal formados etc.

En nuestro caso nuestro firewall es el punto por el que pasan todos los paquetes entre nuestras redes e Internet, así que los paquetes pueden ser analizados y bloqueados antes de entrar en nuestra red, Snort no sólo revisa qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento ¡maravilloso! La base de datos de firmas de "ataques conocidos", permiten distinguir a Snort entre un buen uso de nuestra red o un ataque desde o hacia nuestras máquinas.

Para activar el IDS seleccione SERVICIOS en el menú de la parte superior de la pantalla y luego INTRUSION DETECTION en el submenú de la izquierda.

En esta pantalla nos encontramos con el interruptor para habilitar o deshabilitar snort, también tenemos unos checksbox para configurar en qué interfaz queremos que esté vigilante, seleccionamos todas las interfaces, nos interesa detectar patrones sospechosos tanto en nuestra red verde, en DMZ como en la interfaz Roja.

Uno de los puntos fuertes de esta versión de Endian es que es capaz de actualizar las "firmas" para detectar ataques automáticamente, programamos la actualización una vez al día, también podemos pulsar el botón para que las actualice ahora y comprobar el correcto funcionamiento, para los usuarios avanzados permite insertar nuestras propias firmas.

Duerma tranquilo: Copias de Seguridad

Es realmente sencillo hacer un backup de nuestra configuración para guardarlo en un lugar seguro. La restauración para recuperarnos tras un desastre, 10 minutos de reinstalar el sistema y 2 para cargar el backup. Haga clic en SYSTEM en el menú superior, en el submenú de la izquierda pulse BACKUP.

Podemos elegir distintos tipos de backup, solamente la configuración, volcado de las bbdd, los ficheros de logs actuales,todos los ficheros de logs y los comentarios, también tenemos la opción de encriptar la copia de seguridad. Pulse en CREATE BACKUP decida qué quiere añadir a la copia y duerma tranquilo.

Conclusiones

Endian Firewall es una completa solución cortafuegos Open Source, es sencillo de instalar, tiene una clara interfaz web para la administración, viene "Out the Box" con muchas funcionalidades, snort, antivirus, proxy, OpenVPN, etc...

Como posibles defectos, probablemente subsanados en la versión de pago, es la defectuosa traducción al español y la falta de un sistema de actualización sencillo para la distribución.

Las pruebas se han realizado sobre la versión 2.2 del software liberada en fecha 2009-06-03, existe una versión superior 2.3 liberada unos meses después, 2009-10-27, que no aconsejamos ya que nos encontramos con varios bugs serios que sólo han sido corregidos en la versión "enterprise" del producto.



En la red

- [1] *http://www.clamav.net/*
- [2] *http://www.squidguard.org/*
- [3] *http://www.snort.org/*
- [4] *http://docs.endian.com/archive/2.2/*
- [5] *http://efwsupport.com/*
- [6] *http://sourceforge.net/projects/efw/files/Development/*
- [7] *http://es.wikipedia.org/wiki/Network_Address_Translation*
- [8] *http://www.squid-cache.org/*
- [9] *http://en.wikipedia.org/wiki/Platform_for_Internet_Content_Selection*
- [10] *http://docs.endian.com/archive/2.2/efw.vpn.html*
- [11] *http://es.wikipedia.org/wiki/PKCS*



Sobre los autores

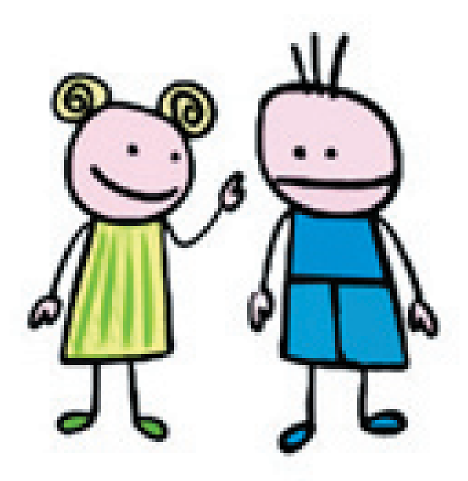
Isabel María Carrasco Martínez es Profesora Técnica de Servicios a la Comunidad en Murcia, Educadora Social especializada en el uso de las Nuevas Tecnologías en la educación, apasionada por el software libre y su aplicación con fines sociales.

Alfonso Vera Rubio es Ingeniero Técnico en Informática, Administrador de Sistemas Linux en Oesía y colaborador en proyectos sociales basados en software libre.

De Claroline a Mentor

Antonio Gómez García, María Dolores Nogueras Atance

La ya inevitable irrupción de las TIC en nuestra sociedad obliga a nuestro sistema educativo a adaptarse a los nuevos tiempos y a incorporarlas como una herramienta más de comunicación de contenidos y de evaluación de resultados. En las siguientes líneas, aprenderemos a instalar en nuestro servidor la plataforma CLAROLINE y a adaptarla a la idiosincrasia particular de un centro de educación secundaria.



En efecto. Incluso los más reticentes a admitirlo, no han podido encontrar más excusas para afrontar la innegabilidad de la irrupción de las Tecnologías de la Comunicación y de la Información no ya en el sistema educativo, que al fin y al cabo es, en parte, sólo un reflejo de la sociedad dentro de la que está realizando su tarea, sino en la vida en general, sea desde el punto de vista del ocio, laboral, social, político, etc... Pero también es cierto que es muy necesaria una adecuada planificación de la inclusión de estas herramienta en nuestro diario quehacer pedagógico. No podemos dar la razón a los más agoreros, y hacer de las tecnologías informáticas herramientas *sustitutivas*, más que *complementarias*, de las tradicionales. La presencia del profesor y la comunicación verbal, la retroalimentación, el trabajo individual, grupal, la realización de pruebas prácticas en aquellas materias que así lo tengan estipulado... todo ello sigue siendo muy necesario.

Pero también es necesario incorporar, no como anécdota, sino como un método de trabajo común, la utilización de ordenadores al diario proceso de enseñanza-aprendizaje, con dos objetivos fundamentales:

- De cara al propio proceso de enseñanza-aprendizaje: enriquecer la aprehensión de contenidos y la evaluación de resultados, desde el punto de vista del aprendizaje significativo: si el niño puede experimentar la utilidad de los conceptos con los que está trabajando, será más sencillo que los retenga y los utilice para mejorar su autonomía y aprender otros conceptos relacionados, normalmente más complejos.
- De cara a la inserción social de un joven que necesita formarse como ciudadano: en el futuro, la utilización de plataformas como las que vamos a ver hoy serán de uso común, tanto para realizar trámites de tipo administrativo, como en el marco laboral, e incluso de ocio común. La incorporación, desde cortas edades, de rutinas como mantener una dirección de correo electrónico de la que responsabilizarse, conociendo las pautas básicas de protección, o de registrarse en determinados servicios que exigen precisamente una



Figura 1. En www.claroline.net, está toda la información necesaria sobre la plataforma, además de la última versión libre para descargar

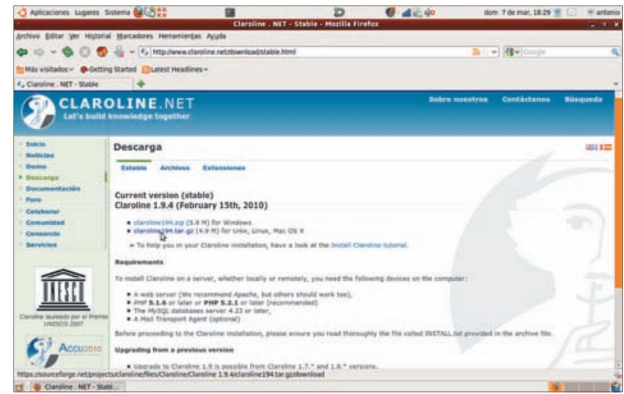


Figura 2. Los requerimientos para que nuestro hosting pueda trabajar con la plataforma son fáciles de satisfacer, y pueden verse en su mismo sitio web

dirección de e-mail, supondrán un aprendizaje útil (más un fin que un medio) en el futuro próximo de los alumno.

Los educadores con cierta experiencia que estén leyendo estas líneas estarán, posiblemente, pensando algo parecido a esto: "*Vale. Otro gran pedagogo que se llena la boca con palabras como aprendizaje significativo, evaluación de resultados, TIC... Pero luego esto en el día a día de mi clase, ¿cómo podría reflejarse? ¿Debe un profesor ser, además de formador, psicólogo, canguro, amigo, educador, rector, guía espiritual... también un ingeniero informático?*".

Bueno, la respuesta es que no, claro. De hecho, quienes esto están escribiendo, ni siquiera son profesionales de la Informática, sino que llevan años en el día a día del aula. Es precisamente por el enfrentamiento de ambos puntos de vista, por el que estamos apostando por la adaptación de algunos formatos, en el marco del software libre, orientados a la formación a distancia, normalmente en el marco de la educación superior, pero que están resultando sorprendentemente adaptables a nuestras circunstancias. Nos referimos, en este caso, a la plataforma Claroline. Más concretamente, vamos a relatar una experiencia que se está realizando dentro de un IES, un instituto de educación secundaria, en Castilla la Mancha (España), más concretamente el Eduardo Valencia de Calzada de Calatrava, en Ciudad Real. Este mismo centro ha protagonizado artículos anteriores sobre la implementación de un servidor global con Ubuntu, que precisamente alojará en su servidor web dicha plataforma, que hemos bautizado como Proyecto MENTOR.

¿Por qué Claroline?

En el seno de la educación pública en España, dos formatos distintos están acaparando la mayor parte de las experiencias en enseñanza: Moodle y Claroline. Originalmente, Moodle parece más potente y propicio al trabajo en educación secundaria, al mostrarse más potente y acomodaticio (en un principio) a la transmisión de contenidos, presentación de trabajos, estética de los documentos... mientras que Claroline puede resultar más estático e inamovible (también en un principio).

Sin embargo, los docentes con experiencia en centros, compartirán con los redactores de este artículo el siguiente convencimiento: *todas las experiencias con TIC en centros educativos se suelen acometer con júbilo y entusiasmo al principio, los ánimos se enfrían a los primeros inconvenientes, y normalmente al final de la experiencia, es difícil que la mitad, ni siquiera un tercio, o un cuarto, o un quinto... bueno, lo más normal es que sólo los emprendedores que diseñaron el intento mantengan la experiencia como parte de su quehacer educativo diario*.

¡Cuidado! No queremos pecar de pesimistas. Simplemente, debemos afrontar que el profesor, desde el punto de vista profesional, tiene ya muchos frentes que acometer, como para tratar de formarse de motu propio en unas tecnologías que exigen muchas horas de dedicación. Es por eso que Moodle puede tener utilidad, pero no es factible su utilización cuando queremos que el profesorado se implique en la introducción de contenidos, pruebas teóricas y prácticas, etc... en nuestra plataforma.

Claroline, en cambio, no exige más que unos conocimientos a nivel de usuario de informática. El profesor ni siquiera tiene que saber qué es un servidor, una base de datos MySQL, o el lenguaje PHP. Se conecta con su nombre de usuario y contraseña, comprueba el trabajo de sus alumnos, e introduce nuevos contenidos.

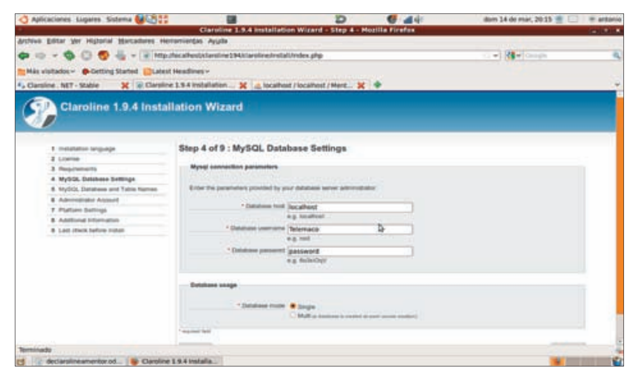


Figura 3. Los pasos de instalación no son muy complejos, pero es imprescindible tener preparada la base de datos MySQL y el usuario con privilegios para usarla correctamente preparados

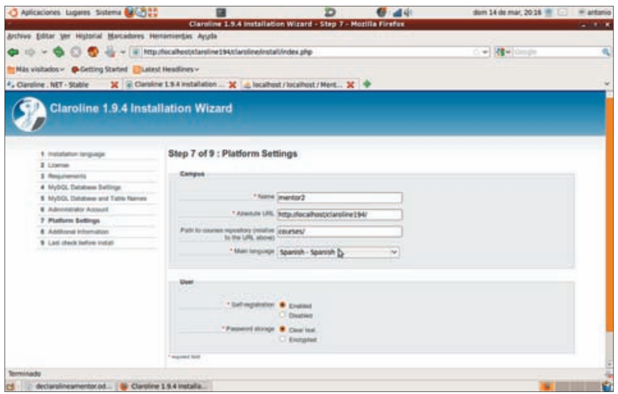


Figura 4. Si bien empezamos trabajando en Inglés, Claroline puede configurarse para funcionar en Español en el séptimo paso de instalación

Descarga e instalación de Claroline

Claroline puede descargarse libremente de la dirección *http://www.claroline.net.* En el momento de redactar estas líneas, va por la versión 1.9.4., y está disponible tanto para Windows como para Linux/Unix. Ya hemos comentado que en este caso, disponemos de un servidor dedicado instalado y mantenido desde la comunidad, pero incluso en institutos y/o colegios en que no cuentan con tal herramienta, como suele ser común, cuentan normalmente con un espacio web, privado o facilitado por la administración educativa, donde dicha plataforma puede alojarse.

Los requisitos son simples, y la mayoría de los espacios web cuentan ya con ellos: debe contarse con la versión 5 del lenguaje PHP, trabajar con bases de datos de tipo MySQL (recomendable contar con la herramienta PHPMyAdmin), y, opcional pero aconsejable, contar con un MTA (Mail Transfer Agent, Agente de Transferencia de Correo). Incluso muchos servicios de hosting gratuitos de corte publicitario cumplen con estos requisitos.

Al tratarse Claroline de un sistema gestor de contenidos, al estilo de Joomla! o Wordpress, e incluso MediaWiki (el motor de la famosa Wikipedia), necesitaremos tener definida una base de datos en nuestro servidor, asignada a un usuario creado específicamente para tal fin (es muy desaconsejable trabajar siempre con un usuario *root* con acceso a todas las bases de datos), que cuente con todos los permisos de lectura, escritura y creación de tablas.

De todos modos, toda esta información se ofrecerá al usuario cuando descargue la última versión de la plataforma, en la sección *Descargas* de dicho sitio web (véase Figura 2).

Trabajemos en nuestro servidor, o utilicemos un espacio web de pago o gratuito, los siguientes pasos se repetirán del mismo modo:

- Descargamos la última versión de la plataforma del sitio *http://www.claroline.net.*
- Descomprimimos (viene en formato **.tar.gz*).
- Subimos mediante un servidor FTP a nuestro espacio web (*Filezilla* es el cliente de mejor resultado para los redactores del artículo).
- Nos aseguramos de contar con los datos de la base MySQL y usuario MySQL (en el caso de tener un servidor propio, se realiza muy fácilmente mediante la herramienta PHPMyAdmin, cuya instalación se ha explicado en los números de enero y febrero de 2010 de esta publicación).
- Nos conectamos mediante nuestro explorador web a la dirección en que hemos instalado la herramienta, y vamos siguiendo las instrucciones.

El Listado 1 nos permitiría descargar e instalar la herramienta desde consola.

A continuación, debemos asegurarnos de contar con una base de datos y su correspondiente usuario, que alojará las tablas en las que se irá introduciendo y ordenando toda la información. Supongamos, por ejemplo, que el nombre de la base sea Mentor y el usuario con derechos Telemaco. Como ya se ha dicho, dependiendo del tipo de servicio web con que se cuente, dichos elementos nos vendrán dados o los generaremos nosotros a partir de PHPMyAdmin. En el caso de nuestro servidor dedicado, al que tenemos pleno acceso, esta tarea puede realizarse desde consola (véase el Listado 2). ¡Ya está todo preparado para la instalación! La dirección web a la que nos dirigiremos será aquella en la que estamos trabajando, seguida de /claroline/install/ en nuestro ejemplo, *http://www.mipaginadeformacion.com/claroline194/claroline/install.*

A partir de ahí, los pasos a seguir son muy intuitivos:

- Seleccionamos idioma (al principio, el español no está disponible),
- Aceptamos las condiciones de la licencia GNU que se nos ofrece,

Listado 1. Descarga y primera instalación de Claroline en nuestro servidor Apache

```
administrador@granhermano:sudo su
:cd /var/www
administrador@granhermano: wget https://
sourceforge.net/projects/claroline/files/Claroline/
Claroline%201.9.4/claroline194.tar.gz/download
administrador@granhermano: tar -xvf
claroline194.tar.gz
```

Listado 2. Creación de la base de datos Mentor y asignación de derechos a usuario Telemaco

```
administrador@granhermano: mysql -u root -p

Enter password: ······
Welcome to the MySQL monitor.  Commands end with ;
or \g.
Your MySQL connection id is 480
Server version: 5.1.37-1ubuntu5.1 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear
the current input statement.

mysql>CREATE DATABASE `Mentor`;
mysql>CREATE USER `Telemaco`;
mysql> CREATE USER 'Telemaco'@'localhost' IDENTIFIED
BY 'password';
mysql> GRANT ALL PRIVILEGES ON Mentor.* to
'Telemaco'@'localhost' IDENTIFIED BY 'password' WITH
GRANT OPTION;

(Se entiende que password sería la contraseña
especificada por el administrador)
```

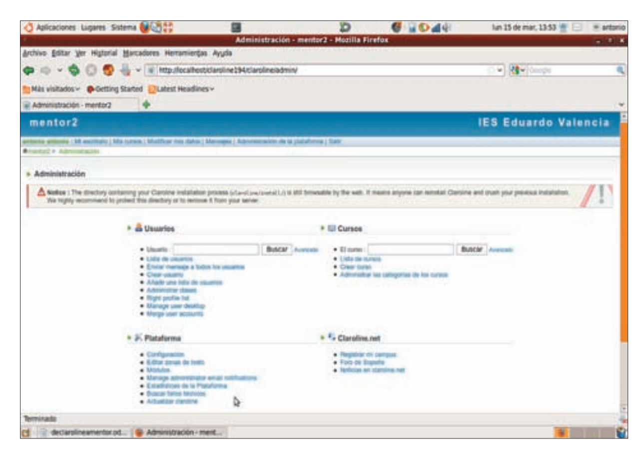


Figura 5. Sólo el Administrador tendrá acceso a este apartado de configuración general de Claroline (dentro del Proyecto Mentor para nuestro centro)



- El sistema comprueba que cumplimos los requerimientos (muchas veces, algunas condiciones aparecen en rojo, pero si nos permite seguir, quiere decir que sólo son recomendaciones),
- Indicamos nombre de usuario y password, así como el nombre de la base de datos MySQL (Figura 3),
- Se nos indicará que dicha base de datos ha sido previamente creada. Debemos marcar la opción de que conocemos esa condición, y que realmente queremos utilizar dicha base de datos,
- En sitios web que alojen varios gestores CMS que estén obligados a compartir base de datos, para que sus respectivas tablas no entren en conflicto, es costumbre nombrarlas a partir de prefijos que señalen su origen. En el caso de Claroline, el prefijo es cl_, si bien el usuario puede especificar otro prefijo,
- Indicamos el nombre de login, el password, e-mail y datos del administrador de la plataforma (o sea, nosotros),
- Terminamos introduciendo la información adicional. Concretamente, el paso número 7 es el que nos permite, ahora sí, cambiar a español como lengua nativa,
- Al finalizar la instalación, la plataforma estará disponible en la dirección web que habíamos dispuesto para ella, si bien se nos recomienda que borremos o renombremos la carpeta */claroline/install* en el directorio.

De Claroline a Mentor: adaptando la plataforma a nuestro centro

El comienzo será común para cualquier institución educativa: el administrador se identificará en la plataforma, después de lo cual se le ofrecerán, en el menú superior, opciones adicionales que le permitirán configurar la plataforma a la realidad de su instituto o escuela (opción *Administrar la plataforma*, véase la Figura 5).

Normalmente, el administrador será también profesor del centro, por lo que también ya podrá crear sus propios cursos. Las opciones de configuración general para el Administrador de la Plataforma se organizan en torno a seis grandes grupos de posibilidades:

- USUARIOS: desde aquí se puede acceder a toda la información de los usuarios registrados en Mentor, crear y borrar usuarios, administrar las clases, etc...
- PLATAFORMA: este grupo de opciones permite configurar la plataforma como tal: editar zonas de texto comunes a todas las clases, configurar módulos, revisar las estadísticas de acceso, consulta y edición a lo largo del curso para todos los usuarios, e incluso actualizar la plataforma.
- HERRAMIENTAS: información del sistema.
- CURSOS: desde aquí se pueden crear cursos a los que el usuario común se puede suscribir, y consultar datos sobre cursos ya creados.
- CLAROLINE.NET: podemos registrar nuestra plataforma de formación, y acceder tanto a foros de soporte como a distintos grupos de noticias.

Comenzamos a trabajar. Jerarquía de usuarios

Una vez ya está lista la plataforma para funcionar, se irá construyendo entre todos los miembros de la comunidad. Para ello, cada profesor o alumno que acceda por primera vez a la plataforma educativa, deberá registrarse, para lo que tendrá que introducir un nombre de login y una contraseña que le identificarán y autenticarán, además de otros datos personales, que el administrador puede configurar desde su perfil.

El administrador (admin, originalmente) de la plataforma es el que irá concediendo los distintos perfiles a cada usuario; según el perfil que se obtenga, aparecerán o no determinadas opciones de configuración dentro del curso en el que se está trabajando.

- *Anónimo o invitado*: el que no está registrado o está registrado pero no se ha matriculado en el curso en cuestión. Lo más normal es que se le deniegue el acceso a cada curso, o se le permita acceso sólo a algunas partes del curso (Documentos, Ejercicios,...). En nuestro centro, normalmente, se permite acceso a la sección de Documentos, pero no a Trabajos, Ejercicios, Anuncios o Agenda.
- *Usuario*: usuario registrado que se ha matriculado en un curso creado por un Coordinador.
- *Coordinador*: usuario al que el Administrador le ha concedido este perfil. Puede crear cursos libremente, permitir el acceso libre o mediante contraseña a sus cursos, programar trabajos y baterías de ejercicios, acceder a toda la estadística de los usuarios matriculados en sus cursos,... Originalmente, será cada profesor del centro registrado en la plataforma.
- *Administrador*: como ya hemos dicho, es el profesor responsable de la plataforma. Es conveniente que sólo haya uno por centro.

Estructura básica de un Curso

Al crear un curso, el Coordinador puede decidir si permite libre acceso o exigirá contraseña al resto de usuarios para acceder al total o a una parte del curso, o especificar derechos de acceso separando



Figura 6. Éste es el aspecto general de un curso cuando un Usuario autorizado (matriculado), accede a dicho curso

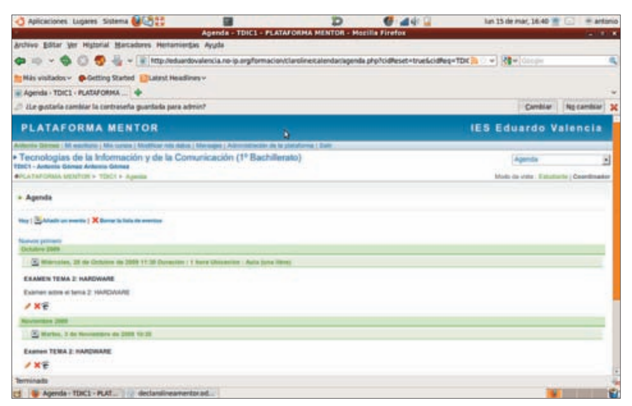


Figura 7. En nuestro IES, un servicio de agenda puede ser muy útil cuando el alumno tiene que tener en cuenta no sólo fechas de exámenes, sino también posibles recuperaciones, entrega de trabajos, etc...

a Invitados, Anónimos y Usuarios. Al terminar de configurar dicho curso, cada Usuario podrá *Matricularse en el Curso en cuestión*, lo que le granjeará el acceso al curso.

Dentro de cada Curso, el Usuario podrá utilizar varios servicios.

Descripción del curso

Editado por el Coordinador, se trataría de un texto (se permiten imágenes e incluso vídeos) descriptivo de los objetivos, contenidos y criterios de evaluación a aplicar a lo largo del curso.

Agenda

Los Usuarios (registrados y matriculados) disponen de un servicio de Agenda, regentado por el Coordinador, en el que se irán introduciendo los Eventos previstos (exámenes, celebración de prácticas, excursiones, etc...) para el Curso en el que estamos. Al autenticarse, los usuarios serán avisados de que se ha producido una novedad en la agenda, cuando ésta se produzca.

Anuncios

En este apartado, se podrán registrar anuncios varios, no relacionados con ninguna fecha en el tiempo, pero que interesa comunicar a la clase. Desde este apartado pueden enviarse también mensajes a uno o varios usuarios, que recibirán en su cuenta de correo electrónico.

Documentos

Este es uno de los apartados más útiles para el profesorado, puesto que pueden colgar varios documentos, organizados, si así se desea, en carpetas, para poner a disposición de los alumnos. Eso sí, debe tenerse en cuenta que cada Coordinador tiene derecho a una cierta cuota de disco en el servidor (ocho megabytes, por defecto, si bien también se puede configurar este aspecto). La tónica más común, en nuestro centro, es preparar los documentos con OpenOffice.org, y luego aprovechar su característica de exportación a formato PDF, a todas luces el más cómodo de transmitir, por su universalidad y pequeño tamaño de los archivos obtenidos. Puede colgarse cualquier tipo de documentos, incluidos enlaces a otras páginas, e ¡incluso! Imágenes de otras web, o vídeo embebido tipo You Tube.

Ejercicios

En este apartado, el Coordinador puede ir fabricando su propia batería de ejercicios y/o preguntas, contando con una gran gama de posibilidades: ejercicios de respuesta múltiple, relación, rellenar huecos, verdadero/falso,... Al poder establecer una respuesta para los grupos de preguntas que se preparen, el Usuario podrá acceder a un servicio estadístico en el que se le informe de sus progresos en relación a la resolución de dicho grupo de preguntas, dado que es la propia plataforma la que evalúa al Usuario, independientemente del Coordinador. Éste, por su parte, tendrá acceso a las estadísticas de todos los alumnos matriculados.

Secuencia de aprendizaje

A partir de los Documentos y los Ejercicios/Preguntas creados en los apartados anteriores, el Coordinador puede establecer una Secuencia de Aprendizaje, consistente en ir insertando, a modo de módulos, dichos elementos en un orden determinado. El estudiante, al ir accediendo a cada módulo (Documento, Ejercicio o Pregunta), e ir satisfaciéndolo, pasará al módulo siguiente. Una estadística registrará los accesos del estudiante a cada módulo, para información tanto del propio Usuario como del Coordinador.

Trabajos

El profesor puede encargar trabajos de investigación, redacción,... en determinadas condiciones a su alumnado. Al acceder a cada Trabajo encargado por el Coordinador, el Usuario puede encontrarse con que se le pida un texto a rellenar en un formulario de tipo Text Box, que agregue su trabajo como un documento adjunto, o ambas opciones. El Coordinador, como en todos los otros aspectos del Curso, puede establecer fechas de plazo tope, condiciones en que cada tipo de Usuario puede acceder a los Trabajos, y decidir si los trabajos de cada alumno serán o no públicos para el resto de sus compañeros. A la entrega de cada Trabajo, el profesor (Coordinador) puede evaluarlo y asignarle una nota en forma de porcentaje, que la plataforma comunicará al alumno en cuestión.

Foros

La plataforma cuenta, a su vez, con un sistema simple, pero muy potente y accesible para todos, de foros. Igualmente se puede establecer si el acceso a los Foros es público y libre, o de tipo restringido en su lectura, escritura o ambos.

Grupos

El profesor Coordinador puede establecer dos o más grupos de alumnos dentro de la misma clase, al objeto de dividir el trabajo por partes,

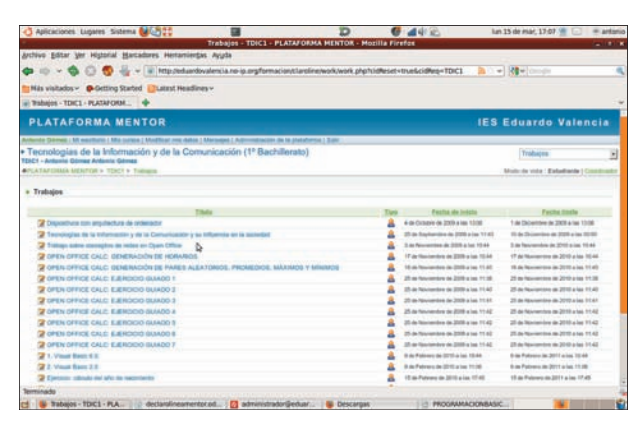


Figura 8. En Educación Secundaria, empieza a ser común encargar trabajos de investigación en formato electrónico, obviando el papel. Mentor recoge los trabajos y comunica a cada alumno la nota que el profesor ha puesto a su actividad

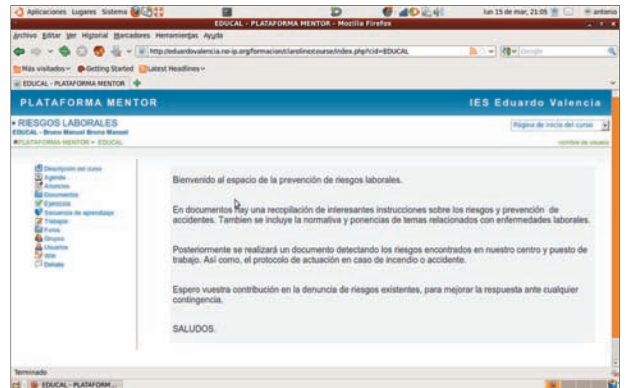


Figura 9. Mentor se está mostrando útil también como punto de encuentro para otras actividades, fuera de las del carácter educativo, que se llevan a cabo en la comunidad



establecer grupos de prácticas, etc... Los alumnos dentro de un mismo grupo podrán ser afectados por órdenes o mensajes colectivos por parte del profesor.

Usuarios

Como ya se comentaba en apartados anteriores en el caso del Administrador, el profesor Coordinador tendrá acceso a todos los datos de los alumnos matriculados en su curso desde este apartado, pudiendo incluso enviarles mensajes de e-mail de manera sencilla y directa.

Wiki

No podía faltar una herramienta tan potente y versátil en una plataforma educativa que reúne, en muchos aspectos, las características de una auténtica red social. El uso de una wiki, al estilo de la famosa Wikipedia, como hilo conductor de un trabajo colaborativo de investigación, puede potenciar la motivación del alumnado a la hora de participar en las actividades de enseñanza-aprendizaje programadas.

Debate

Se trata simplemente de un curioso, sencillo pero efectivo servicio de chat en PHP al servicio de los alumnos que coincidan en el tiempo en el mismo curso de la plataforma. Una herramienta más de comunicación, al mismo tiempo que de motivación, para el alumnado, que pueden "quedar" a través del servicio de Agenda, o incluso de Anuncios, con compañeros del mismo o distintos grupos. Para contactar desde su propia casa para colaborar en la redacción de un trabajo, respuestas a baterías de ejercicios, intercambio de documentos, etc...

Recapitulando

Hasta ahora, hemos visto cómo se instala una plataforma basada en Claroline, preparando la base de datos MySQL y su respectivo usuario, los primeros pasos de configuración, y la estructura básica de un Curso. En este último apartado ha podido verse la razón de que en un instituto de Educación Secundaria suela resultar preferible a otros sistemas como el famoso y no menos válido Moodle, dado que su utilización por parte del profesorado no exige conocimiento previo alguno de programación, gestión y administración web, o redes. Los conceptos que caracterizan y singularizan a Claroline, resumiendo, serían los siguientes:

- El usuario principal es el *Administrador*, que concede permisos de Coordinación a los usuarios que sean profesores.
- Los *Coordinadores* crean y personalizan sus cursos, en los que deben matricularse los *Usuarios* registrados.
- Todas las secciones de todos los Cursos son editables y configurables por el responsable correspondiente, sea éste *Administrador* o *Coordinador*. Para ello, una vez se ha identificado como tal, sólo tendría que hacer clic en *Editar esta zona de texto*.
- El *Coordinador* de cada curso puede establecer qué partes del curso serán visibles o invisibles para cada tipo de usuario. En suma, sanciona los permisos de lectura y escritura de cada apartado del curso para los alumnos.
- Cada vez que se produce una novedad, sea del tipo que sea (nuevos eventos en la Agenda, nuevos documentos sin consultar por parte del alumno, un alumno ha entregado un trabajo que el profesor aún no ha consultado, etc...), se avisa al usuario al conectarse por medio de un punto rojo al lado del apartado en que se ha producido dicha novedad.
- Cada *Curso* consume una cuota de disco en el servidor en que se encuentra alojado, que puede modificarse por parte del *Administrador*.

Conclusiones

Si bien siempre habrá profesores que encuentren algún motivo para mantener alejados sus métodos pedagógicos de las Nuevas (que ya no son tan Nuevas) Tecnologías, Claroline está demostrando ser una herramienta muy potente y versátil. Su principal atractivo es su facilidad de instalación, amén de estar en idioma español, y lo amigable del interfaz de usuario. Por otro lado, la gran cantidad de herramientas en forma de módulo que se ofrecen en cada curso, no tienen por qué suponer un motivo de avasallamiento para el usuario novel, toda vez que tanto Administrador como Coordinadores pueden establecer qué módulos serán visibles y cuáles no. Concretamente, en nuestro IES, el Eduardo Valencia de Calzada de Calatrava (Ciudad Real), tan atractiva está resultando esta plataforma que algunos profesores la están utilizando no solamente como herramienta educativa, sino también como medio de comunicación y propagación de protocolos y normativas, como está siendo el caso del profesor Coordinador de Riesgos Laborales del centro, que utiliza a Mentor como plataforma de lanzamiento de toda la documentación que se genera (prevención de riesgos, ergonomía, planes de evacuación, etc...).

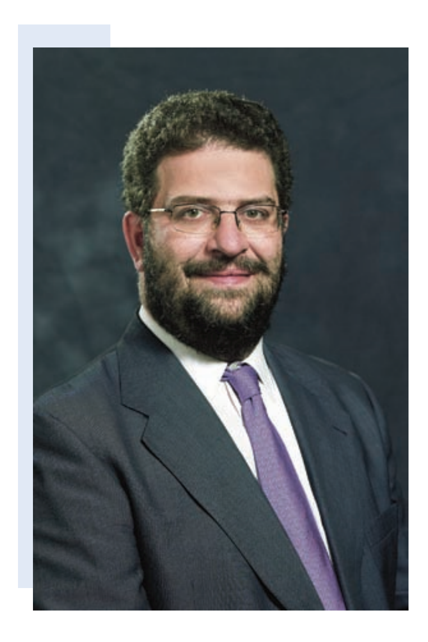
Resumiendo, y retomando lo que decíamos al principio del artículo, lo que nació como una plataforma de E-Learning más orientada a la educación superior, es muy útil como complemento (repetimos, nunca sustituto) de la actividad diaria del profesor en un entorno de enseñanza-aprendizaje. El ahorro de papel, por otro lado, es otro motivo más para tener en cuenta la posible utilización en un centro de esta herramienta, puesto que los centros educativos, no ya consumen, prácticamente *fagocitan* el papel, con las consecuencias medioambientales que todos conocemos. La motivación del alumnado, la versatilidad de toda la estadística de acceso y evaluación de actividades a que puede acceder cada profesor, son sólo argumentos para rematar la justificación del experimento realizado, que en los meses de curso que llevamos, ha demostrado cumplir, y superar, todas nuestras expectativas.



Sobre los autores

Antonio Gómez García es Ingeniero Técnico Industrial de Formación, y va ya para diez años que dedica su actividad profesional a la Educación Secundaria y Bachillerato en institutos. Profesor de Tecnologías y de Tecnologías de la Información, ha trabajado como asesor TIC en el Centro de Profesores de Puertollano, y dedica gran parte de su tiempo al software libre y su introducción en el sistema educativo. En la actualidad, es Responsable de Medios Informáticos en el IES Eduardo Valencia, de Calzada de Calatrava (*Ciudad Real*).

María Dolores Nogueras Atance, licenciada en Ciencias Químicas, es también profesora de Tecnologías, después de pasar algunos años como profesora de Formación Profesional en Laboratorio. Su irrupción en el mundo informático fue algo más tardío, y debido sobre todo a la estrecha relación de dicho mundo con la materia que actualmente imparte. Sin embargo, ha sabido retomar el ritmo y pone a prueba y se esfuerza por aprender toda nueva herramienta informática que caiga en sus manos y que pueda tener algo que ver con la educación.



De vender cajas
a preocuparse por el cliente

Fernando de la Cuadra, director de Educación de Ontinet.com, distribuidor en exclusiva de las soluciones de seguridad de ESET en España

La situación económica en este momento no es la más adecuada (por decir algo suave) para muchísimos distribuidores de productos informáticos. La venta de productos "de consumo" ha caído en picado, y desgraciadamente, muchos pequeños distribuidores están cerrando.

No soy, ni mucho menos, un experto en economía, pero hay un comportamiento que siempre ha sido clave a la hora de servir como último eslabón en la cadena comercial: el producto que se nos está ofreciendo a los clientes. En muchas ocasiones, los fabricantes consiguen que un producto entre en el mercado a través del canal sin tener en cuenta al mismo canal. Las personas que están en contacto con nosotros, los sufridos consumidores, se convierten entonces en unos meros vendedores de cajas.

Aunque hayan cerrado muchos distribuidores, veo con alegría que la inmensa mayoría de los que sobreviven no se dedicaban únicamente a cambiar cajas de sitio. Efectuaban una venta, es decir, se molestaban por que tuviéramos lo que realmente buscábamos, y nos lo ofrecían del fabricante que tuviera ese producto o que se preocupara por el distribuidor. No es poner una caja y abrir el monedero: es preocuparse, cuidar al cliente.

Esa tarea se vuelve muy difícil cuando lo que estás haciendo no es un asesoramiento a la hora de montar una red, ni estás buscando el software de facturación que mejor se adapta a esa empresa o a ese cliente que ha entrado por la puerta pidiendo lo más extraño que te puedas imaginar. Ese cliente ha pedido, precisamente, "una caja". Necesita un producto que no es más que un software empaquetado, ya "listo para su consumo".

¿Dónde queda entonces la labor del distribuidor? Pues precisamente en saber elegir qué cajas va a tener. No es solo saber si el producto es bueno, sino saber qué fabricante va a preocuparse por el cliente tanto como el distribuidor.

Que el fabricante no solo "venda cajas" es tan importante como que el distribuidor no lo haga. El trabajo no puede recaer únicamente en el distribuidor, no es posible hacer un trabajo si el fabricante no va a responder con las mismas ganas y la misma intensidad. Un distribuidor necesita que el cliente tenga detrás también al fabricante, dispuesto a ayudar, dar soporte, formar… Vamos, lo que hace años se llamaba "atención al cliente" y ahora se resume en tener una página web con un teléfono 806 de contacto.

Nosotros, los clientes, buscamos una rentabilidad en la inversión, y la obtendremos cuando descubramos que una caja tiene muchomás que cartón. Que tiene a un profesional detrás, preocupado porque el producto sea el más adecuado para nuestras necesidades. Y tiene a un fabricante detrás, que no le dejará "colgado" cuando le necesite y que se va a ocupar, también, del cliente. Es decir, de nosotros.

Páginas recomendadas


www.diariolinux.com


www.elguille.info


www.gatolinux.blogspot.com


www.opensourcespot.org


www.hispabyte.net


http://sliceoflinux.com/


www.linuxhispano.net


www.pillateunlinux.wordpress.com


www.usla.org.ar


www.mundopc.net


www.picandocodigo.net


www.linuxuruguay.org



CONCURSO UNIVERSITARIO DE SOFTWARE LIBRE

FASE FINAL

13 Y 14 DE MAYO

ESCUELA DE INGENIERIA DE LA UNIVERSIDAD DE CADIZ

CHARLAS SOFTWARE LIBRE

PRESENTACION DE PROYECTOS

ENTREGA DE PREMIOS

PATROCINADOR PRINCIPAL



PATROCINADOR ORO



PATROCINADOR PLATA



PATROCINADOR BRONCE



COLABORADOR PRINCIPAL



COLABORA





















MEDIOS OFICIALES







LiNUX+

ORGANIZA

